[19]中华人民共和国专利局

[51]Int.Cl[6]
G06K 9/00

[12] 发明专利申请公开说明书

[21] 申请号 96195641.0

[43]公开日 1998 年 8 月 19 日

[11] 公开号 CN 1191027A

[22]申请日 96.5.17

[30]优先权

[32]95.5.17 [33]US[31]08 / 442,895

[86]国际申请 PCT / US96 / 07185 96.5.17

[87]国际公布 WO96 / 36934 英 96.11.21

[85]进入国家阶段日期 98.1.19

[71]申请人 斯马特·塔奇公司

地址 美国加利福尼亚州

[72]发明人 尼德·霍夫曼 戴维·F·佩尔
乔纳塞恩·A·李

[74]专利代理机构 中国国际贸易促进委员会专利商标事务所

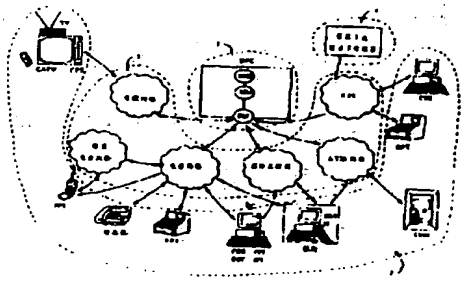
代理人 鄢 迅

权利要求书 9 页 说明书 144 页 附图页数 20 页

[54]发明名称 用于电子交易和电子传输授权的无代价券识别系统

[57]摘要

一种无代价券的识别系统和方法，主要基于对从未知用户直接收集的比如指纹或声音记录这样的唯一生物特征采样与先前获得并存储的相同类型的验证生物特征采样进行相关比较（1）。可将其连到网络中，起到其他独立计算机系统（3）之间的完全或部分中介作用，或者可以是执行全部所需任务的单独计算机系统。



权 利 要 求 书

1.自动的无代价券识别计算机系统，用于通过对在尝试步骤中收集的至少一个生物特征采样和一个个人识别代码进行检查、并且与在登记步骤中收集的先前记录的生物特征采样和个人识别代码进行比较，来确定个人的身份，所述系统包括：

a. 至少一个计算机；

b. 第一收集和显示装置，用于在登记步骤中自动输入来自于个人的至少一个生物特征采样、个人识别代码和专用代码，其中专用代码是由个人选择的；

c. 第二收集和显示装置，用于在尝试步骤中自动输入来自于个人的至少一个生物特征采样和个人识别代码；

d. 第一互连装置，用于将所述第一和第二收集和显示装置互连到所述计算机，以便将所收集的生物特征采样、个人识别代码和专用代码从所述第一和第二收集装置传送到所述计算机；

e. 用于对在尝试步骤中收集的生物特征采样和个人识别代码与在登记步骤中收集的生物特征采样和个人识别代码进行比较，以便产生一个估值；

f. 位于所述计算机中的执行装置，用于存储数据和处理及执行命令，以便产生一个确定；以及

g. 用于从所述计算机输出所述估值、确定和专用代码的装置。

2. 根据权利要求 1 的装置，其中计算机包括用于检测和避免计算机系统的电子入侵的装置。

3. 根据权利要求 1 的装置，其中计算机远离收集和显示装置放置。

4. 根据权利要求 1 的装置，第一和第二收集和显示装置还包括：

a. 用于收集生物特征采样的至少一个生物特征输入装置，还包括一个硬件和软件部件；

b.在功能上部分或完全地与生物特征输入装置集成在一起的至少一个终端装置，用于输入和增加附加数据；

c. 用于输入个人识别代码的至少一个数据输入装置，其中所述装置

或者与生物特征输入装置或者与终端装置集成在一起；以及

d. 第二互连装置，用于互连所述生物特征输入装置、数据输入装置和所述终端。

5. 根据权利要求 4 的装置，其中所述终端还包括至少一个用于显示数据的显示装置。

6. 根据权利要求 4 的装置，其中生物特征输入装置具有一个先前登记在计算机中的硬件识别代码，该代码使得生物特征输入装置对计算机是唯一可识别的。

7. 根据权利要求 4 的装置，其中硬件部件还包括：

a. 至少一个用于数据处理的计算模块；

b. 用于存储数据和软件的可擦和不可擦存储模块；

c. 用于输入生物特征数据的生物特征扫描装置；

d. 用于输入数据的数据输入装置；

e. 数字通信端口；以及

f. 用于避免电子窃听的装置。

8. 根据权利要求 7 的装置，其中各计算机模块以一种方式连接，以避免监测计算机模块之间的通信。

9. 根据权利要求 7 的装置，其中硬件部件还包括用于显示数据的显示装置。

10. 根据权利要求 7 的装置，其中硬件部件还包括射频屏蔽。

11. 根据权利要求 4 的装置，其中硬件部件还包括一个无线通信装置。

12. 根据权利要求 7 的装置，其中生物特征输入装置免于受到物理撞击。

13. 根据权利要求 12 的装置，还包括用于检测对生物特征输入装置的物理侵入的装置。

14. 根据权利要求 13 的装置，还包括用于电子自毁的装置，从而擦除在存储模块中存储的软件和数据。

15. 根据权利要求 13 的装置，还包括物理自毁的装置，从而摧毁计

算模块和存储模块。

16. 根据权利要求 4 的装置，其中硬件部件还包括用于读取磁条卡的装置。

17. 根据权利要求 4 的装置，其中硬件部件还包括用于读取智能卡的装置。

18. 根据权利要求 4 的装置，其中软件部件驻留在计算模块中，并且还包括：

a. 电可擦存储模块，其中存储了至少一个命令接口模块、第一套软件及相关数据，它们被特别配置为专门用于生物特征输入装置和数据；以及

b. 不可擦存储模块，其中存储第二套软件及相关数据。

19. 根据权利要求 18 的装置，所述软件部件还包括用于将数据从明文加密到密文的装置。

20. 根据权利要求 18 的装置，所述软件部件还包括用于检测数据改变的装置，还包括：

a. 一个秘密密钥；以及

b. 一种不可逆单向数据变换，没有秘密密钥时不能再现数据。

21. 根据权利要求 18 的装置，其中第一套软件及相关数据还包括：

a. 生物特征编码算法；以及

b. 加密代码。

22. 根据权利要求 18 的装置，其中第二套软件及相关数据还包括：

a. 一个操作系统；以及

b. 至少一个设备装置程序。

23. 根据权利要求 4 的装置，其中所述终端是任何电子装置，它向生物特征输入装置发出命令并从其接收结果。

24. 根据权利要求 23 的装置，其中所述终端是从传真机、电话、电视远端控制器、个人计算机、信用/借方卡处理器、现金收款机、自动出纳机、无线个人计算机的组中选择的。

25. 根据权利要求 4 的装置，其中所述第二互连装置是用于无线通信的装置。

26. 根据权利要求 1 的装置，其中所述第一互连装置是从 X.25 、ATM 网、电话网、国际互联网、有线电视网、蜂窝电话网的组中选择的。

27. 根据权利要求 1 的装置，其中比较装置还包括用于对数据进行加密和解密的装置。

28. 根据权利要求 1 的装置，其中比较装置还包括用于识别生物特征输入装置的装置。

29. 根据权利要求 1 的装置，其中计算机系统还包括:

a. 至少一个独立计算机网络系统；以及

b. 第三互连装置，用于互连所述计算机系统和所述对方计算机系统。

30. 根据权利要求 29 的装置，其中第三互连装置包括一个 X.25 网络。

31. 根据权利要求 1 的装置，其中执行装置包括至少一个用于存储和检索数据的数据库。

32. 根据权利要求 31 的装置，其中数据库还包括一个个人生物特征数据库。

33. 根据权利要求 31 的装置，其中数据库还包括一个先前欺诈检查数据库。

34. 根据权利要求 31 的装置，其中数据库还包括一个电子文件数据库。

35. 根据权利要求 31 的装置，其中数据库还包括一个电子签字数据库。

36. 根据权利要求 1 的装置，其中所述输出装置是从 X.25 网、 ATM 网、电话网、国际互联网、有线电视网的组中选择的。

37. 根据权利要求 1 的装置，其中所述专用代码是由计算机产生的。

38. 自动地和无代价券地识别个人并且鉴定该识别的方法，所述方法包括下述步骤:

a. 登记步骤，在此收集并存储来自个人的至少一个生物特征采样、个人识别代码和专用代码;

b. 尝试步骤，在此收集来自个人的至少一个生物特征采样和个人识

别代码;

c. 比较步骤，在此对在尝试步骤中收集的生物特征采样和个人识别代码与在登记步骤中收集并存储的生物特征采样和个人识别代码进行比较，以便产生成功或失败的识别结果;

d. 执行步骤，在此对一个命令进行处理并且执行，以产生一个确定;

e. 输出步骤，在此将所述识别结果或确定形象化并且显示; 以及

f. 展示步骤，在此将个人的成功标识、专用代码展示给正被识别的个人。

39. 根据权利要求 38 的方法，其中登记和尝试步骤两者都还包括一介生物特征采样检查步骤，在此验证生物特征采样的质量。

40. 根据权利要求 38 的方法，其中登记步骤还包括一个个人识别代码和生物特征采样双重检查步骤，在此对照当前与相同个人识别代码相关的所有先前登记的生物特征，对在登记步骤中收集的生物特征和个人识别代码进行检查。

41. 根据权利要求 38 的方法，其中登记步骤还包括一个辅助数据输入步骤，在此收集辅助数据。

42. 根据权利要求 41 的方法，其中辅助数据还包括个人的姓名和地址。

43. 根据权利要求 41 的方法，其中辅助数据还包括个人的职别。

44. 根据权利要求 43 的方法，其中辅助数据输入步骤还包括一个职别索引指定步骤，在此对每个个人职别指定一个代码。

45. 根据权利要求 41 的方法，其中辅助数据还包括一个金融资产帐号。

46. 根据权利要求 45 的方法，其中辅助数据输入步骤还包括一个帐户索引指定步骤，在此对每个金融资产帐号指定一个索引代码。

47. 根据权利要求 38 的方法，其中登记步骤还包括一个先前欺诈检查步骤，在此对在登记中收集的生物特征采样与先前登记生物特征采样的一个子集进行比较。

48. 根据权利要求 38 的方法，其中登记步骤还包括一个紧急机制建立步骤。

49. 根据权利要求 48 的方法，还包括一个紧急帐户索引指定步骤，在此将一个帐户索引标记为紧急帐户，该帐户在适当的授权方被通知紧急时得以访问。

50. 根据权利要求 49 的方法，还包括一个假屏幕显示步骤，在此指定假屏幕数据。

51. 根据权利要求 49 的方法，其中对各种金融资产帐户的访问受到限制。

52. 根据权利要求 38 的方法，其中登记步骤还包括一个修改步骤，在此能够修改和删除任何先前输入的辅助数据。

53. 根据权利要求 38 的方法，其中登记和尝试步骤两者都还包括一个数据密封步骤，以提供检测数据改变的能力，还包括:

a. 一个秘密密钥；以及

b. 一种不可逆单向数据变换，没有秘密密钥时不能再现数据。

54. 根据权利要求 38 的方法，其中登记和尝试步骤还包括一个加密步骤，以将数据从明文转换为密文。

55. 根据权利要求 38 的方法，其中登记或尝试步骤还包括一个传输步骤，在此传输数据。

56. 根据权利要求 38 的方法，其中尝试或登记步骤还设有唯一传输入代码，该代码具有唯一硬件识别代码和由每次传输时加一的自增序列号。

57. 根据权利要求 38 的方法，其中登记步骤还包括在一个设置语言步骤中选择一种通信语言。

58. 根据权利要求 38 的方法，其中尝试步骤还包括在一个设置职别号步骤中选择一种职别。

59. 根据权利要求 38 的方法，其中尝试步骤还包括在一个设置帐号步骤中选择一个帐号。

60. 根据权利要求 38 的方法，其中尝试步骤还包括在一个确认量值步骤中确认一个量值。

61. 根据权利要求 38 的方法，其中尝试步骤还包括在一个输入量值步骤中输入一个量值。

62. 根据权利要求 38 的方法，其中尝试步骤还包括在一个确认文件步骤中确认一个文件。

63. 根据权利要求 38 的方法，其中尝试步骤还包括在赋值寄存器步骤中追加辅助数据。

64. 根据权利要求 63 的方法，辅助数据还包括对方识别代码。

65. 根据权利要求 38 的方法，其中尝试或登记步骤还包括在复位步骤中退出或取消所述步骤。

66. 根据权利要求 38 的方法，其中尝试步骤还包括在传输步骤中传输数据。

67. 根据权利要求 38 的方法，其中尝试步骤还包括在设置语言步骤中选择一种通信语言。

68. 根据权利要求 38 的方法，其中比较步骤还包括使用唯一的传输代码以检测重复传输。

69. 根据权利要求 38 的方法，其中比较步骤还包括一个利用对方标识和唯一传输代码的对方识别步骤。

70. 根据权利要求 38 的方法，其中比较步骤包括将在尝试步骤中收集的个人的个人识别代码和生物特征与在登记步骤中收集的个人识别代码和生物特征进行匹配，以便正确识别该个人。

71. 根据权利要求 70 的方法，其中在登记步骤中收集的个人识别代码和生物特征与在尝试步骤中收集的个人识别代码和生物特征不匹配，则不识别该个人。

72. 根据权利要求 38 的方法，其中执行步骤还包括一个借/贷交易步骤。

73. 根据权利要求 72 的方法，其中借/贷交易步骤还包括一个地址收集步骤。

74. 根据权利要求 38 的方法，其中执行步骤还包括一个存档步骤和一个用于获得数据的跟踪代码指定步骤。

75. 根据权利要求 74 的方法，其中通过消息摘要编码算法步骤发送数据，以产生电子签字的文件。

76. 根据权利要求 38 的方法，其中执行步骤还包括利用跟踪代码检

索存档的数据。

77. 根据权利要求 38 的方法，其中执行步骤还包括一个修改步骤，在此增加、删除或修改索引代码、帐号和帐户索引代码。

78. 根据权利要求 38 的方法，其中执行步骤还包括一个帐号检索步骤，在此使用帐户索引代码检索一个帐号。

79. 根据权利要求 38 的方法，其中执行步骤还包括一个紧急活动步骤。

80. 根据权利要求 79 的方法，其中紧急活动步骤还包括识别紧急代码、将整个交易标识为紧急并且通知授权方。

81. 根据权利要求 79 的方法，其中执行步骤还包括一个假显示步骤，在此可以存取先前指定的假帐户或对帐户的假限制。

82. 根据权利要求 38 的方法，其中输出步骤还包括一个识别结果通知步骤。

83. 根据权利要求 38 的方法，其中输出步骤还包括一个确定通知步骤。

84. 根据权利要求 38 的方法，其中输出步骤还包括一个紧急代码步骤，在此通知授权方。

85. 根据权利要求 38 的方法，其中输出步骤还包括一个显示假屏幕的步骤。

86. 根据权利要求 38 的方法，其中展示步骤还包括对专用代码进行加密、形象化和解密。

87. 快速搜索来自第一个人的至少一个第一先前存储的生物特征采样的方法，搜索中采用个人识别代码篮，篮中可以含有来自至少一个第二个人的至少一个算法上唯一的第二生物特征采样，并可由所述个人识别代码篮标识，包括：

a. 一个存储步骤，还包括：

1) 由所述第一个人选择个人识别代码；

2) 输入所述第一个人的生物特征采样；

3) 找到由所述第一个人所选择的个人识别代码所标识的个人识别代码篮；

4) 对取自所述第一个人的生物特征采样与在所述所选择的个人识别代码篮中的先前存储的生物特征采样进行比较，以确定由所述第一个人所输入的生物特征采样是算法上不同于先前存储的由至少一个第二个人提供的至少一个生物特征采样；以及

5) 如果所述第一个人的所输入的生物特征采样在算法上不同于至少一个无前存储的来自所述至少一个第二个人的生物特征采样，则将其存储在所选择的个人识别代码篮中；以及

b. 一个尝试步骤，还包括：

1) 由所述第一个人输入所述所选择的个人识别代码；以及

2) 由所述第一个输入一种生物特征采样；以及

c. 一个比较步骤，还包括：

1) 发现由所述第一个人所输入的所述个人识别代码所标识的个人识别代码篮；以及

2) 对来自所述第一个人的所输入的生物特征采样与所述输入的个人识别代码篮中的所述至少一个第二个人的至少一个所存储的生物特征采样进行比较，以便产生一个或者成功的或者失败的识别结果。

说　　明　　书

用于电子交易和电子传输授权的无代价券识别系统

本发明是1994年11月28日递交的美国专利申请第08/345,523号的部分继续申请，在此引用作为参考。

当今的金融世界流行代价券和信用卡。代价券是任何授予给个人的非生命物体。该物体赋予给呈递该物体的个人一种能力。通过使用代价券或塑料片对每个金融帐户进行远程访问。无论是使用借方卡购买杂货还是用信用卡购买消费物品，交易的核心是代价券允许的资金汇兑，该代价券标识某个个人及其所访问的金融帐户。

从金属币转到使用塑料卡的原因是简单和直接的：在资金汇兑系统中对货币的存取对于商户和消费者来说都远比使用大量硬币和纸币来得安全。

不妙的是，与这种方便的以代价券为基础的资金汇兑系统相结合的技术导致的系统易受到盗窃和作弊。

用户身份的验证仅基于置入代价券的数据，该数据易于在不同的个人之间复制和转移。这样的安全性必须依靠被授权的用户和商户在保持信息专用方面和努力和幸运。但是，由于固有特性，代价券与个人之间没有很强的关联。通过代价券识别该代价券的正当拥有者最大程度上也是脆弱的。从如下事实可以看到这一点：代价券的正当拥有者之外的个人曾使用这种代价券欺骗商户和其他消费品供应者。

八十年代消费者信用业的很大发展给发卡者带来了很大利润并给消费者带来了新的便利。但是，由于消费者信用对于消费者来说容易获得，它成为犯罪者的目标。就象在20年代和30年代初汽车移动性导致大量的银行抢劫一样，消费者信用的普及导致了犯罪机会的增加。

最初，银行业接受由于欺诈导致的部分损失并把代价转嫁到消费者身上。但是，由于犯罪变得越来越有组织。技术越来越高，并且信用零售站

开始由越来越没有受到信用卡安全方面训练的人经营，欺诈造成的损失的增长率激增。欺诈的惊人的统计数字和防范步骤的代价迫使信用卡公司专门寻找其他解决方案。

信用卡工业的欺诈损失起源于信用卡系统高度脆弱本性的很多不同的方面，但主要原因是丢失、被盗和伪造卡。信用卡的操作无需个人标识码（PIC）的使用，因此丢失的卡一旦落入他人之手就可变为金钱。代价券的盗窃占系统中欺诈的大多数，伪造信用卡的使用在上升。伪造卡是由技术上更老练的犯罪者通过获得持卡人的有效帐号并使用该有效帐号制造的。伪造者对磁条进行编码，并用该帐号膜加（emboss）该伪造塑料卡。该卡再被呈递给商户并记入正当持卡人的帐户。另一种形式的损失是由于碰巧得到持卡人帐号的犯罪商户。还有一种类型的欺诈是被授权持卡人所为，在这种欺诈中，先用代价券购买商品，然后宣称该代价券已丢失或被盗。估计每年所有类型的欺诈造成的损失超过九亿五千万美元。

通常，借方卡与个人标识代码（PIC）联合使用。伪造借方卡更困难，因为罪犯不仅必须获得帐号，还要得到PIC，然后象制造信用卡那样制卡。但是，有很多从持卡人获得PIC的方法，如不收现金但记录PIC的购物中心的特洛伊木马自动出纳机或ATM，也记录PIC的商户销售点装置，以及用望远镜观察持卡人在ATM上输入PIC的个人。随后制造的伪造借方卡在各种ATM机器上使用，直至该帐户被用空。

金融业知道欺诈代价的趋势并且不断采取步骤增强卡的安全性。代价券的欺诈和盗窃给系统的造价带来了间接的影响。

空白卡是在很严格的安全条件下制造的。这些卡然后被标以帐号和期满日期并被寄往持卡人。光是制造和分配卡每年要消耗10亿美元。金融业对标准卡的造价是每卡2美元，但这2美元中只有0.3美元是与实际制造成本有关。

过去10年中，金融业由于伪造及欺诈已改变了代价券，但没有进行信用交易系统的使用的根本性变化。补救措施是行政管理变化，如让用户呼叫发卡行来使它们的卡有效。其他的变化包括增加全息防伪、照片ID或改进的签字区域。这些类型的变化表明系统对欺诈的敏感性在于缺乏个人的真正识别。估计每年这可造成制造造价倍增到20亿美元。

在较近的将来，银行业预计将转向更昂贵的卡，即“智能卡”．智能卡包含与一些第一家用计算机同样的计算能力。第一代智能卡的现在的造价计划估计在大约为每卡 3.5 美元，并不包括分配费用，这将明显高于塑料空白卡的 0.3 美元的造价。

造价的明显增加已迫使金融业除了简单的交易授权之外寻找使用智能卡的能力的新方式。可以看到，在存储贷方和借方帐号之外，智能卡还可存储电话号码、经常飞行里数、从商店得到的优惠券、交易的历史、在收费厅和公共交通系统可使用的电子化币、以及用户的姓名、关键数据甚至是病历。显然，金融业的趋势是进一步建立代价券的使用。

智能卡的能力的增加的副效应是功能的集中。功能增加的副面效应是增加的脆弱性。有了智能卡的这些功能，这种高档卡的丢失或损坏将给持卡人带来巨大的不便。没有这样一个卡将使持卡人在财务上无能为力，直至替换该卡。另外，丢失一个装满电子货币的卡也将导致真正的财务损失。另外，尚未提及每天可复制一张智能卡的伪造能力。

不妙的是，由于智能卡上显现的功能集中，持卡人更易受到卡本身丢失或损坏的影响。于是，在花了大量的钱之后，完成的系统更安全，但在消费者身上对这种卡的损坏或丢失有可能受到越来越重的惩罚。

金融业认识到了与智能卡有关的安全性问题，并进行努力以使每个塑制卡难以伪造。数以几十亿计的美元在今后五年以被用于使塑制卡更安全。至今，消费者金融交易业有一个平衡的简单公式：为了减少欺诈，必须增加卡的造价。

与电子金融交易的普及有关并在此之外，广泛使用了电子传真、电子邮件消息和类似的电子通信．对金融交易中个人的适当识别的缺乏的问题与电子传输中个人的适当识别的缺乏是类似的。电子通信的方便和快速以及与普通邮递相比的低价是个人之间以及商业界的通信方式的一个选择。这种类型的通信已有很大增长并预计会继续增长。但是，如传真和电子邮件（或称“E-mail”或称“email”）的百万计的电子消息被传送但不知道它们是否到达了真正的目的，或者不知某人是否真的发送或收到该电子消息。另外，也无法验证发送或接收电子消息的个人的身份。

最近，许多努力用于克服代价券和代码安全系统中的内在问题。一个

主要的方面是对PIC进行加密、改变或修饰，使得未经授权的用户更难于进行多于一次的交易，很大程度在于处理PIC以使这种代码更能抵制欺诈。已提出了许多方法，例如引入一种算法，该算法以一种仅使用者知道的方式改变PIC，使得每下一次对帐户的访问需要一个不同的PIC码。例如，PIC码可被改变并被订成专门对于访问试图的日历日或日期。在另一种方式中，引入了时间可变因素以产生一个可预测的个人标识码，该码在访问的时间仅对被授权的使用者显示。虽然更不易被欺诈，系统包含了不变码，这样的方法不是实质上免于欺诈的，因为它仍依赖于并不是对于被授权用户个人而言是唯一的和不可再造的数据。另外，这样的系统对于不易记住不变代码及少变代码的消费者来说是不方便的。这些方法的例子在授予Dethloff等的美国专利4,837,422，授予Weiss的美国专利4,998,279;授予Weiss的美国专利5,168,520;授予Mosley的美国专利5,251,259；授予Parrillo的美国专利5,239,538；授予Martino等的美国专利5,276,314和授予Goldfine等的美国专利5,343,529中被公开，所有这些专利在此引用作为参考。

在更近的时间里，有人把注意力从使用个人标识代码转向使用唯一的生物特征数据作为身份验证和最终的计算机访问的基础。在这种方式，从有已知身份的用户记录下真实的生物特征数据并存在代价券上以备将来查证。在每一个随后的访问试图中，要求用户以物理方式输入所要求的生物特征数据，所输入数据与代价券上的鉴别生物特征数据相比较以确定两者是否匹配以验证用户身份。因为生物特征数据对用户个人是唯一的，并且以物理方式输入生物特征数据是实质上不可再造的，一种匹配可推定实际身份，因此减小了欺诈的风险。建议了许多生物特征数据，如指纹、手纹、声纹、视网膜像、手写笔迹采样等。但是，由于生物特征数据一般以电子方式存储（因而可以再造）在代价券上并且比较和验证过程并不脱离于由试图访问的个人直接使用的硬件和软件，欺诈访问的显著风险仍然存在。系统安全的这种方式的例子在以下专利中被描述：授予Lafreniere的美国专利4,821,118，授予Piosenka等的美国专利4,993,068；授予Lilley等的美国专利4,995,086；授予Uchida等的美国专利5,054,089；授予Barbanell的美国5,095,194;授予Yang的美国美国5,109,427;授予Igaki

等的美国专利 5,109,428；授予 Kobayashi 等的美国专利 5,144,680；授予 Higuchi 等的美国专利 5,146,102；授予 Hiramatsu 的美国专利 5,180,901；授予 Lee 的美国专利 5,210,588；授予 Usui 等的美国专利 5,210,797；授予 Fishbine 等的美国专利 5,222,152，授予 Fishbine 等的美国专利 5,230,025；授予 Horie 的美国专利 5,241,606；授予 Bush 等的美国专利 5,265,162；授予 Heath, Jr 等的美国专利 5,321,242；授予 Knapp 的美国专利 5,325,442；授予 Willmore 的美国专利 5,315,303，所有这些专利在此引用作为参考。

从以上讨论可以理解，存在巨大的和不可避免的需求来试图设计高度抵制欺诈的安全系统，但对于消费者很容易使用并且很方便。不利的是，如上所公开的对代价券和代码系统的所建议的改进没有涉及，更没有试图平衡这种需求。这样的系统通常把被鉴定的生物特征数据以电子形式直接存储在可以被认为是可被复制的代价券上。另外，这样的系统不能使身份验证过程适当地隔离于试图获得非授权访问的人的介入。

一个以代价券为基础的依赖用户的生物特征数据的安全系统的例子可以在授予 Gullman 等的美国专利 5,280,527 中找到。在 Gullman 的系统中，用户必须携带并呈递一个信用卡大小的代价券（被称为生物特征数据安全装置），该代价券包含一个微芯片，在该微芯片上记录了被授权用户声音的特征。为了启动访问程序，用户必须将代价券置入如 ATM 的终端，然后对终端说话以提供生物特征数据输入来与被呈递的代价券的微芯片上的鉴别的输入相比较。身份验证的过程通常并不能与试图进行非授权访问的人的介入相隔离。如果有了匹配，远程终端可通知主计算机访问应被允许，或在向主计算机发送必需的验证信号前可以提示用户输入附加的代码，如 PIN（也存储在代价券上）。

虽然 Gullman 系统中的存储的与输入的生物特征数据的比较与数字码相比减小了非授权访问的风险，Gullman 使用代价券作为鉴定数据的存储体的做法以及 Gullman 的无法使身份验证过程与介入的可能性相隔离这个缺点减少了由生物特征数据代替数字码后抵制欺诈的任何改进。另外，由于还需要呈递一代价券来启动访问请求，该系统有些笨拙并且不方便。

几乎是一致地，公开以代价券为基础的系统的专利没有揭示在不使用

代价券的情况下对生物特征数据的识别。这种作法的原因涉及生物特征数据识别系统的存储需要，以及识别大量个人的显著时间延续，甚至对最大型的计算机也如此。

从前面的情况看，长期以来需要一种计算机访问系统，它能高度抵制欺诈，实用而且有效率地便于用户操作并且迅捷地进行电子交易与传输。

还需要一种计算机系统，该系统完全是无代价券的并且能验证用户的个人身份。这种验证只是基于个人识别代码和在物理性质上对被授权用户具有唯一性的生物特征数据，这些都不同于验证某个人是否具有可以在不同的个人之间可自由传递的物体。这样的生物特征数据必须易于并无损伤地获得，必须易于并低价存储和分析，并且不必侵犯个人隐私权。

计算机访问系统设计的进一步需要是用户的方便性。非常希望消费者能自发地访问系统，特别是非预计的需要产生时，而只需最少的努力。特别地，需要系统极大地降低或消除记忆大量或累赘的代码的必要，并且使得不必携带并呈递独有的物体来启动访问请求。

这样的系统必须操作简单、精确并且可靠。需要一种计算机访问系统，它能够允许用户访问多个帐户并且获得授权给用户的所有服务，进行所有金融帐户内以及帐户间的交易，支付购物费用以及收到各种服务，等等。

还有更大的需要，就是需要一种计算机访问系统，它能给予被授权用户以下这种能力：向授权方报警：一个第三方正强迫用户请求访问而不让第三方知道已产生报警。还需要一种系统，它能在使进行强迫的第三方不知道的情况下对访问一旦被准许时对可以进行的交易的类型和数量进行暂时的限制。

另外，该计算机系统必须是可以买得起的并且足够灵活，使得能与具有各种电子交易和传输装置及系统结构的现有网络兼容地运行。

最后，需要电子邮件消息和电子传真的安全发送与接收，电子消息的内容被保护而不公开给未被授权的个人，能以很高的确定性获得发送方和接收方的身份。

本发明通过提供改进的识别系统来满足这些需要，该改进的识别系统用于通过将在一个在尝试步骤中收集的一个个人的生物特征数据采样和个人识别代码与在一个登记步骤中为该个人收集并存储在数据处理中心的远

程站 点中的生物特征数据采样和个人识别代码进行比较以确定该个人的身份。本发明包括一计算机网络主系统，该系统具有用于比较输入的生物特征数据采样和个人识别代码的装置，并配备有各种数据库和存储模块。另外，本发明配备有生物特征数据与个人识别代码输入装置以及当个人的身份被确定时用于输入数据来提供由主机执行的被请求交易和传输的信息的装置。本发明还配备有用于连接主计算机与终端及生物特征数据输入装置的装置。

该计算机还配有用于除了传统的存储数据与修改之外还执行各种交易和传输的装置。另外，该计算机能输出生物特征数据－ PIC （“个人识别代码”）比较的评估，以及一个识别评估的确定，或者交易或传输的任何执行的状态。另外，该计算机系统对被验证的个人进行通知并进行鉴别，表明该计算机系统被访问，这些是通过向个人发送回一个在登记步骤中该个人先前选择的专用代码来完成的。

该计算机系统最好受到保护而免于电子窃听和电子入侵与病毒。另外，这些由计算机使用来收集生物特征数据采样和个人识别代码的装置包括： a) 至少一个用于收集生物特征数据采样的生物特征数据输入设备，它有一软件部分和一硬件部分； b) 至少一个与生物特征数据输入装置在功能上部分地或完全地集成在一起的用于输入任何附加的辅助信息的终端设备； c) 一个用于输入个人识别代码的数据输入设备，这个数据输入设备与生物特征数据输入设备或终端设备两者之一集成在一起，以及 d) 一个用于互连生物特征数据输入设备、数据输入设备和终端的装置。终端设备还至少有一个用于显示数据和信息的显示器。为了更高的安全性，计算机系统唯一地识别生物特征数据输入设备，并通过与生物特征数据输入设备相连的终端相关的一个柜台方（ counter party ）或商户识别代码唯一地识别柜台方或商户。生物特征数据输入设备最好受到保护而免于物理或电子介入，并且当该设备有物理缺损时，最好采取措施从物理上和/或电子上损坏该装置中的有关部件和/或从该设备的存储器模块中删去关键数据。

另外，生物特征数据输入装置包括硬件部分，该硬件部分包括： a) 用于数据处理的至少一个计算模块； b) 用于存储数据和软件的可擦除或不可擦除存储器模块； c) 用于输入生物特征数据的生物特征数据扫描设备； d)

用于输入数据的数据输入设备； e)一个数字通信端口； f)用于防止电子窃听的设备。

为了保护生物特征数据输入装置、终端以及计算机网络之间的电子数据的完整性和隐蔽性，数据最好被加密并被密封。

主计算机网络以常规方式被连接到其他独立的计算机系统、数据库、传真机和其他计算网络并可与它们通信。

本发明的方法包括自动识别某个个人而不使用任何代价券，识别是通过对该个人提供的至少一种生物特征数据采样和同样由该个人提供的个人识别代码进行检查而完成的。在一登记步骤中，该个人将一个鉴定的生物特征采样、一个个人识别代码和一个专用代码登记到系统中。之后，在一个尝试（bid）步骤中收集该个人的生物特征数据采样和个人识别代码并与在登记步骤中登记的这些内容比较。个人识别代码和生物特征数据采样的匹配导致该个人的肯定识别。为了向被识别的个人认可真正的计算机系统被访问，将在登记步骤收集的专用代码返回给该个人。

本发明的方法最好包括在登记时检查生物特征数据采样的方法并把这样的生物特征数据与被认为试图犯罪或实际上在系统上进行过欺诈的人的生物特征数据采样的集合进行比较。

在一个优选的实施例中，本发明最好包括向授权方通告紧急情况和被授权方处于强迫状态的方法。

最好采用加密和密封数据的方法来保护数据，包括数字化的生物特征数据采样，使数据免于偶然泄漏或在传输过程中由于犯罪因素导致泄漏。

该方法最好包括使个人选择不同的金融帐户并选择不同的电子传输模式的步骤。

该方法最好包括实现数据及电子传输以及使用跟踪代码检索数据的方法。

更好地是，如传真或电子邮件消息的任何文件通过使用算法对其唯一地计算检查和以用于文件将来的识别。

再有，本发明的另一方法是能够通过在一个电子篮（basket）中存储不同个人的若干不类似的生物特征数据采样来检查该个人的生物特征数据采样及个人识别代码来迅速识别该个人，该电子篮由一个个人识别代码标

识。

在本发明的一个实施例中，计算机系统允许个人从由远程数据处理中心选择的一组个人识别代码（PIC）中选择自己的个人识别代码。这是按如下完成的；一旦个人的生物特征数据被收集，数据处理中心随机选择便于记忆的若干个PIC。数据处理中心然后将收集的生物特征数据与那些已在PIC篮或组中的生物特征数据相比较。当新登记者的生物特征数据与已被分配给那些任选的PIC组中的任一个的任何先前登记的生物特征数据相似时，数据库拒绝该PIC被新的个人使用，另一个PIC被选择用于另一次这种生物特征数据比较。一旦数据处理中心收集了若干PIC可选组而没有含混的相似生物特征数据，这些PIC被呈递给新的登记者，从中个人可选择一个PIC。

在本发明的一个实施例中，有一种方法，该方法快速搜索来自第一个个人的至少一个第一个先前存储的生物特征数据采样，使用一个个人识别代码篮，该篮能包括来自至少一个第二个个人的至少一个算法上唯一的第二生物特征数据采样，并且该第二生物特征数据采样由所述个人识别代码篮标识，该方法包括：首先，一个存储步骤，该存储步骤还包括：a)由第一个人选择一个专用代码；b)由所述第一个个人选择一个个人识别代码；c)输入所述第一个个人的生物特征数据采样；d)确定由所述第一个个人选择的个人识别代码所标识的个人识别代码的篮的位置；e)对从所述第一个人获得的生物特征数据采样与在所述被选择的个人识别代码篮中的任何先前存储的生物特征数据采样进行比较以确定由所述第一个个人输入的生物特征数据采样是算法上唯一的并且不同于由至少一个第二个个人提供的先前存储的至少一个生物特征数据采样，以及；f)如果所述采样在算法上唯一且不同于来自所述至少一个第二个个人的至少一个先前存储的生物特征数据采样的话，在所选择的个人识别代码一篮中存储输入的生物特征数据采样。还有一个尝试(bid)步骤，该尝试步骤还包括：a)由第一个个人输入所述所选择的个人识别代码，以及；b)由所述第一个人输入生物特征数据采样。还有一个比较步骤，包括：a)找到由所述第一个人输入的所述个人识别代码所标识的个人标识代码－篮；b)对由所述第一个个人所输入生物特征数据采样与在所述输入的个人识别代码－篮中存储的来自所述至少一

个第二个个人的所述至少一个所存储的生物特征数据采样进行比较以产生一个成功或失败的识别结果。还可以有: a)一个执行步骤，其中一个命令被处理并被执行以产生一个确定; b)一个输出步骤，其中所述识别结果或所述确定被外部化并被显示，以及; c)一个呈现步骤，其中当所述第一个个人的识别成功时向所述第一个个人呈现专用代码。

根据本发明的一个实施例，主系统串接地处于被识别个人与要访问的其他计算机网络之间，因而相当于一个接口。应当理解，在这个实施例中，用户直接向本发明的主计算机系统提出访问请求，该系统与其他独立的安全计算机系统（如VISANET－维萨网）交互操作。该计算机系统因此对它所服务的每个安全计算机系统的所有被授权用户保存鉴定的生物特征数据采样。这些数据由每个被授权用户交互查阅。于是，在身份识别完成后，安全系统向用户提供诸系统的列表，该个人被授权访问这些系统，并向用户提示来选择所希望的网络。于是，类似于当今在商户与信用卡公司之间发送的通信类型，所请求的执行步骤与涉及交易的信息被送至所选择的独立计算机网络。

在第二个实施例中主系统可完成其他独立计算机系统的功能，如对金融帐户的借或贷。在这种系统中，本发明的计算机系统完成由个人请求的功能而无需外部的独立计算机网络。

根据本发明的又一个实施例，提供了一个装置，该装置用于当用户被第三方强迫请求访问主计算机系统时在访问试图中向预先指定的授权方报警。在这个实施例中，被授权用户有几个代码，绝大多数被计算机系统识别为标准访问代码，其他的被识别为紧急代码。本发明的计算机系统的比较装置可被配置成对每个被授权用户接受和识别至少一个代码，只要由用户输入的代码与紧急代码匹配就启动紧急报警装置。同时，对于用户的被授权身份的确定导致用户可在也许是预定的受限制的访问级别上访问被请求的安全计算机系统或导致误导数据（即“假屏幕”），因此防止强迫他人的第三方知道用户已输入了紧急通知。紧急代码的输入可以作为用户个人识别代码的一部分或与用户个人识别代码同时输入，或者，在访问计算机系统时选择一个紧急帐户索引。在每种情况下，如果强迫方发现用户正试图通知授权方，则请求访问的用户的安全就有危险。因此，很关键的是

访问过程不间断地继续进行并且允许被授权用户访问，使得强迫方相信一切都在正常运行。虽然这些特征可以包含在本发明的主计算机网络中，某个独立的计算机网络也可完成同样的或修改的上述特征。

本发明与现有技术相比在几个方面有明显的优点。首先，它对用户很方便且极富有效率，尤其是在访问金融帐户时，因为它不要求携带并呈递任何代价券以访问某人的帐户。本发明免除了与携带、安全保存和放置任何需要的代价券相关联的所有不便，另外，由于代价券经常是专门用于某个特定计算机系统的，还需要记忆分配给该特定代价券的密码，本发明通过只使用一个个人识别代码来提供对所有资产的访问显著地减少了需要消费者投入的记忆和精力。因此，在一个单一的、无代价券的交易中，消费者可高效率和安全地进行实质上任何商业交换或电子消息交换，如从银行帐户取现金，偶然同术语的授权同意，从电视上直接购物以及支付地方财产税。消费者依靠本发明目前拥有了独特能力，可方便地在任何时间进行个人和/或职业的电子传输和交易更不必依靠可能被盗、丢失或损坏的代价券。

本发明有一个显著的优点是方便，使零售商和金融机构在做买卖及进行另外金融交易时少一些麻烦，多一些便利。与当前系统相比，可以显著降低金融交易中的纸件工作，例如当前的信用卡购买系统需要分别产生供信用卡公司、商户和顾客使用的收据。这种电子交易极大地降低了操作成本，为商户和银行节省了相当的时间和花费。因为本发明的系统使消费者能同时直接访问他所有的金融帐户，显著地减少了涉及货币、支票、商业票据等的交易，从而减少了用来收集及处理这类交易所需的设备及人力。另外，可以基本上消除发行和重发行信用卡、ATM卡、电话卡等卡的制造和发行费用，从而进一步节约了商户、银行的经济成本，并最终节约了消费者的钱。实际上，由于所有的消费者都只要输入它的指纹或其他生物特征数据就能得到它们的电子金融资源，本发明的系统很可能促进经济增长。

本发明的显著优点及超越于现有系统之处是很高的抗欺诈能力。如上所述，当前计算机系统的不可靠性是固有的，因为它们把对用户身份的确定基于一个唯一制造出来的物理形态，在某些情况下，还基于用户知道的

信息。不幸的是，代价券和信息都会由于丢失、被盗或授权用户的主动行为而让他人知道。这样，除非授权用户认识到并报告这些物品的丢失或不经意的传播，拥有这些物品的任何人都能被现存的安全系统识别为被分配了该代价券和信息的授权用户。

相反，本发明对用户的一个或多个唯一的生物特征数据特征进行分析而确定用户身份，实际上消息了授予非授权用户访问的危险。即使在极端的情况下，一个授权用户被强迫方强迫去访问自己的帐户，系统预先能产生一个紧急帐户索引，从而授权用户能在强迫方未察觉的情况下将侵害告知授权方

本发明通过在操作上与请求访问的用户无关的系统中的一点维持鉴别数据并执行身份验证操作，进一步提高了抗欺诈能力，从而防止了用户获取鉴别数据的备份或防止用户窜改验证过程。这样一个系统显然优于现存基于代价券的系统，现存系统中验证信息，例如专用代码存在代价券中并能从代价券中恢复，并且现有系统中实际的身份确定是用户在访问过程中能通过操作而接触的。

因此，本发明的目的是提供一个计算机访问识别系统，它不需要用户为了启动一个系统访问请求而要拥有或提供一个物理物体，例如代价券。

本发明的另一目的是提供一个计算机访问识别系统，与验证拥有专有物体和信息相反，它能验证用户身份。

本发明还有另一目的是基于一个或多个物理上依赖于用户个人的一个或多个独特特征来验证用户身份.

本发明还有另一目的是提供一个实用、方便、易用的安全访问系统。

本发明还有另一目的是提供一个安全访问计算机系统的系统，它对非授权用户的访问尝试有很高的抗欺诈能力:

本发明还有另一目的是提供一个计算机访问识别系统，它使用户能通知授权方一个特定的访问请求是被第三方强迫的，而所述第三方却不知道该通知。

人们还需要一个计算机访问识别系统，能根据用户自己提供的所需配置自动限制该用户在该计算机系统上的交易能力。

参照附图阅读了下面的本发明的详细描述后，本发明的这些及其他优

点将会更清楚。

图 1 为本发明的系统示意图;

图 2 为数据处理中心（ DPC ）及其内部数据库和执行模块的示意图;

图 3 为零售销售点终端、生物特征数据输入装置及其部件以及互连情况的示意图。

图 4 是生物特征数据输入装置和生成请求包的终端的操作流程图;

图 5 是请求包以及它包含的必备数据和可选数据的代表性示意图;

图 6 是应答包以及它包含的必备数据和可选数据的代表性示意图;

图 7 是表示生物特征数据输入装置所进行的数据加密和密封处理的流程图;

图 8 是表示 DPC 所进行的数据解密和柜台方识别处理的流程图;

图 9 是表示 DPC 所进行的数据加密和密封处理的流程图;

图 10 是表示在登记过程中所完成的用户登记的流程图;

图 11 为表示个人识别并且向其返回一个专用代码的处理流程图;

图 12 为 DPC 中所发生的处理及执行步骤的概要流程图;

图 13 为 DPC 中的紧急请求和应答处理的流程图;

图 14 为 DPC 中所进行的零售交易授权处理的全部操作的流程图;

图 15 为 DPC 中所进行的远程交易授权处理的全部操作的流程图;

图 16 为 DPC 中所进行的 ATM 帐户访问处理的全部操作的流程图;

图 17 为 DPC 中所进行的发行人批修改处理的全部操作的流程图;

图 18 为 DPC 中所进行的保密传真提交和电子文件提交处理的全部操作的流程图;

图 19 为 DPC 中所进行的保密传真数据和电子文件数据处理的全部操作的流程图;

图 20A 是电子签字请求包的代表性示意图;

图 20B 是电子签字应答包的代表性示意图;

图 20C 是电子签字验证请求包的代表性示意图;

图 20D 是电子签字验证应答包的代表性示意图;

图 21 为 DPC 中所进行的电子签字处理的全部操作的流程图;

图 22 为 DPC 中所进行的电子签字验证处理的全部操作的流程图。

如上所述，本发明的主要目的在于一种出于进行商业交易或非金融往来而对个人进行识别的能容纳大量用户的无代价券、保密、可靠、安全并且是可协调的装置和方法。本发明的精髓在于，顾客无需使用任何的代价券、信用卡、标记或者识别卡（包括驾驶执照）就具有进行这些交易的能力。为了能够达到实用化，很重要的一点是系统要以完成金融交易（如从多家银行和多个信用卡帐户完成信用卡购物和 ATM 服务）所需要的速度工作。系统还必须安全，无论在进行个人识别和授权交易的计算机系统内还是在与计算机系统进行通信的计算机系统和远端站之间的数据传送期间，客户的个人记录和他们的生物特征数据必须保密、安全。另外，系统还必须可靠，识别和授权中的错误必须不能妨碍系统运行或者使系统的使用变得麻烦。由于计划只使用生物特征数据来识别个人，系统还必须具有在紧急情况下或者降低（甚至是授权用户的）访问等级或者通知授权方的保安措施。此外，该系统还必须能够处理大量的用户，适合于对大量数据（如生物特征信息）进行存储和传送，并且适应当今社会中金融交易的处理速度。

现在来看附图。图 1 示出了本发明的总体结构及各个组成部分。其本质是，一个数据处理中心（ DPC ） 1 通过各种各样的通信装置 3 （可以是几种类型中的一种）连接到各种各样的终端 2 上。该 DPC 还与一个独立的计算机网络 4 相连，并与之进行通信。 DPC 具有如图 2 所示的多个数据库和软件执行模块。在本发明的最佳实施例中，数据库出于安全原因被备份或“镜象”处理。防火墙计算机 5 负责防止对系统的电子入侵，网关机 6 则负责执行来自用户的所有请求，包括对所有的数据库进行增加、删除或者修改。网关机还负责对来自终端的数据使用 MACM 模块 7 、 MDM 模块 8 和 SNM 模块 9 进行解密和解包。 PGL 模块 10 和 IML 模块 11 被用来查找正确的个人识别码和生物特征数据采样篮（ basket ）。图 3 示出了一个终端及生物特征数据输入装置 12 。该输入装置 12 具有一个生物特征数据扫描仪 13 、一个数据输入装置（如数字键盘或 PIN 键盘） 14 及一个显示面板 15 。虽然下面将使用指纹扫描仪作为例子，生物特征数据扫描仪可以是指纹扫描

仪、声音识别装置、掌纹扫描仪、视网膜扫描仪或类似装置中的任何一种。该生物特征数据输入装置还设有计算模块16、设备驱动器和可擦或非可擦式存储模块。生物特征数据输入装置最好通过一个串口 17 与终端进行通信。终端 2 使用图 1 中示出 的一种互联装置如电缆网络、蜂窝电话网络、电话网络、国际互联网、 ATM 网络或 X.25，通过一个常规的调制解调器 18 借助于请求包 19 和应答包 20 与 DPC 进行通信。图 4 示出了请求包 19 及其通过生物特征数据输入装置软件的生成方法的代表性示意图。图 5 和图 6 示出了具有可选和必备数据段的请求包和应答包的代表性示意图，此外还示出了这些包的哪些部分被加密，哪些包被密封。图 7 是对数据进行加密和密封的全部处理的方框图，图中示出了在使用一个消息鉴定代码密钥（ MAC ） 21 密封请求包之前，使用 DUKPT 密钥数据 20 在加入附加数据之前对数据进行加密。图 8 和图 9 示出了在 DPC 中进行的解密和加密处理。图 12 至 19 、图 21 至 22 中的方框图示出了从 DPC 的执行步骤中选出的一些例子。

下面对本发明的附图、示意图、流程图以及发明具体内容如硬件部分、软件部分、执行模块、数据库、连接装置及它们之间的传送的数据进行详细描述。

1.1. 生物特征数据输入装置（ BIA ）

1.1.1. 引言

BIA 是硬件和软件的结合，其职能是收集生物特征数据输入，并对其进行编码和加密，以用于个人识别。 BIA 的所有操作均由一个称为终端的外部控制机构所指示，该外部控制机构通过 BIA 的串行线发出命令，接收结果。

BIA 硬件有 4 种标准形式：标准型、无线型、集成的电话/有线电视（ CATV ）/传真型、和 ATM 型。 BIA 硬件的每一个变型都针对着市场上的某个特定的需要，由于结构不同，每个变型的保密级别也不同。

BIA 软件有 7 种标准形式：个人计算机（或称 PC ）型、零售商型、 ATM 型、登记型、内部型、发行人型和集成远端型。每个软件装入后都提供了一种不同的、专用命令集。举个例子来说，登记软件装入后就不接受形成

零售交易消息的请求。同样，零售软件命令集不能送出个人登记消息。为了提供另一层保护， DPC 了解在每个 BIA 中装入了什么软件包。当一个 BIA 试图发出一个通常不能发出的信息时，会遭到拒绝，会被当作主要安全侵犯。

本发明鉴别和抵御商业欺骗的能力基于下面的事实: 即 BIA 的外部接口是严格限制的， BIA 的结构也使得篡改它的内容变得异常困难，每个 BIA 具有只有 DPC 才知道的独特的加密码，每个 BIA 只被允许执行限于其指定功能之内的操作。每个生物特征数据输入装置具有一个预先存储在 DPC 中的硬件识别码，这使得生物特征数据输入装置在进行每次后续的生物特征信息输入装置传输时都能被 DPC 唯一地识别。

本发明中的 BIA 在构建时基于这样的假设: 即控制终端是欺骗和欺诈之源。终端的范围可以是从运行在个人计算机上的软件应用程序直至为每个专门用途（如商业零售点）开发的专用硬件/软件系统。无论其具体类型如何，没有一个 BIA 能够显示出未经加密的生物特征数据。那些不设显示装置（如 LCD 、 LED 或石英屏幕）的 BIA 必须向终端披露一些选定的信息（如个人专用代码）以供显示，因此，这种特定的终端－ BIA 组合被认为不够安全。

取决于要完成的工作的种类的不同，各种类型的 BIA 要么部分要么全部地和终端集成在一起。部分集成的装置物理上与终端是分离的，它们包括无线型 BIA 和用于商业零售点的标准 BIA 。完全集成的装置被设置在终端（如 ATM 或电话机）自带的机械外壳中。

没有一台 BIA 会向任何外部源透露任何机密的加密代码。

1.1.2. BIA 类型

具体的 BIA 硬件类型具有多种不同的结构。下面对它们作简要介绍。

BIA

标准型具有计算模块（即多芯片模块），生物特征数据扫描仪（即单指纹扫描仪），显示装置（即 LCD 屏），通信端口（即串行口），装在防撞机箱中的数据输入装置（即人工数据输入键盘或 PIC 键盘）以及电子检测装置（即 RF 屏蔽）。

BIA/无线型

标准型，但使用外部天线的广谱无线通信模块取代串行线。用于餐馆等销售点。

BIA/ATM 型

设有重负载型扫描仪、串行口和一个多芯片模块。但由于 LCD 是终端而不是 BIA 的一部分，它必须向终端提供专用代码，故使安全性降低。用于 ATM 中。

BIA/有线电视型

设有轻负载型扫描仪，其他则与 ATM 型类似。用于电话、CATV 远端和传真机中。安全性最差。原因在于一是 LCD 和 PIC 键盘都是终端的一部分而不是 BIA 的一部分，二是由于这个市场中存在的低价格特性。

1.1.3. BIA 命令集消息

每个 BIA 软件命令集都提供了一组不同的操作。下面对它们进行简要介绍。

BIA/ATM

帐户访问

BIA/有线电视

远程交易授权

BIA/传真

保密传真提交

保密传真数据

保密传真跟踪

保密传真检索

保密传真拒绝

保密传真文档

保密传真合同接受

保密传真合同拒绝

电子文件文档检索

BIA/内部

用户识别

BIA/发行人

发行人批处理

BIA/个人计算机

电子文件提交

电子文件数据

电子文件跟踪

电子文件检索

电子文件拒绝

电子文件文档

电子文件文档检索

电子签字提交

电子签字校验

远程交易授权

网络凭证

保密连接

BIA/登记

个人识别

生物特征数据登记

BIA/零售

交易授权

1.1.4. BIA 硬件: 标准型

标准 BIA 硬件是与单纹扫描仪、 LCD 屏幕、 串行口和包覆在一个防撞硬外壳中的 PIC 键盘结合在一起的多芯片模块。上述外壳为其中的部件提供防撞和射频屏蔽的功能.

以下的这些部件被组合成一个称为“ BIA 多芯片模块”的多芯片模块（这是一种本计算领域内公知的将多个处理器包围在一个物理核中的处理）， 它被构建成能够保护设备之间的通信通路，以免容易地被窃听.

- 串行处理器
- PIC 键盘处理器
- LCD 屏幕处理器
- CCD 扫描仪 A/D 处理器
- 含有闪烁 ROM 和掩模 ROM 的高速 DSP 处理器
- 通用微处理器
- 标准 RAM
- EEPROM

以下的软件包和数据被存储在掩模 ROM 中。掩模 ROM 比其他类型的只读存储器便宜，但比较容易被进行反向工程，不能实现电可擦。为此，我们在这里只存储不重要的、通常可以得到的代码（掩模 ROM 在本计算领域内是公知的）。

- MAC 计算库
- DUKPT 密钥管理库
- （带有 CBC 的） DES 加密库
- 基－ 64 （ 8 位至可打印 ASCII ）转换程序库
- 公共密钥加密库
- 嵌入式操作系统
- 串行线设备驱动程序
- LCD 设备驱动程序
- PIC 键盘设备驱动程序
- 扫描仪设备驱动程序
- 唯一的硬件识别码
- 多语言程序概要文件

以下的标准数据和软件包被存储在闪烁 ROM 中。闪烁 ROM 比较昂贵，但很难进行反向工程，最重要的是可以实现电可擦。所有的更重要的数据都存储在这里。使用闪烁 ROM 是为了试图增加复制一个 BIA 的难度（闪烁 ROM 在本计算领域内是公知技术）。

· 唯一的 DUKPT 未来密钥表
· 唯一的 112 位 MAC 密钥
· DSP 生物特征数据质量确定算法
· DSP 生物特征数据编码算法
· 随机数发生器算法
· 命令功能表

随着 BIA 每次发送信息而增加的信息序列号从 BIA 发送并存储在 EEPROM 中。EEPROM 可以被清除许多次，而且还是非易失的，其内容在电源中断期间还保持有效（EEPROM 在本技术领域内是公知的）。

以下的数据被存储在 RAM 中，RAM 本质上是临时性的，一旦掉电其内容将失去。

· 经编码的生物特征数据寄存器
· PIC 寄存器
· 帐户索引码寄存器
· 职别索引码寄存器
· 量值寄存器
· 文件名称寄存器
· PIC－块密钥
· 消息密钥
· 应答密钥
· 共享对话密钥
· 专用对话密钥
· 8 个通用寄存器
· 堆栈和堆空间

每个多芯片模块都含有一个“一次性写入”的存储器位置，该存储器位置在闪烁 ROM 初始化之后被不可逆转地设置。当试图将软件下载到该闪烁 ROM 中时，首先检查该存储器位置。如果该位置已经被设置，BIA 则拒绝加载。这样，重要的软件和数据密钥只能下载到设备中一次（在制造时）。

当一个交易取消时，所有的寄存器和密钥很显然都被清零。一旦交易

完成，寄存器也将被清除。一旦执行“形成消息”命令时，生物特征数据寄存器、 PIC 寄存器、帐户索引码寄存器与后续处理中不需要的任何加密密钥一起被清除。

很重要的一点是，软件在堆栈变量中不保留寄存器的备份或者密钥（这在本领域内是公知的）。

以下的相关联的硬件部分构成了标准的 BIA 硬件模块:

· BIA 多芯片模块

· CCD 单纹扫描仪

· 电容检测板（本领域内公知）

· 发光 PIC 键盘

· 2 行 40 列 LCD 屏幕

· RF 屏蔽

· 防撞机箱

· 串行连接（最高达 57.6kb ）

· breech 检测硬件（本领域内公知）

· 可选的附属于多芯片模块的热电荷装置（ thermite charge ）（本领域内公知）

用来计算这些值的所有临时存储内容、内部硬件和软件都是保密的，这意味着它们会阻止任何确定它们的当前值或它们的功能含义的企图。这一点对于本发明的保密性而言是非常重要的，正因为它非常重要，使得对 BIA 进行“窃听”更具体地说是收集进行欺骗的装置中所用的生物特征数据 - PIC 块变得非常困难，几乎不可能。

在实际装置中，多芯片模块和各部件互相物理地连接在一起而不露出连接线。

保护 BIA 的电子部件的机箱在制造时就被焊死，在任何情况下，不对外壳造成较大的破坏是不可能打开的。当检测到外壳打开（或损坏）时，BIA 对驻留在闪烁 ROM 中的任何或者说所有密钥及随后的全部软件库进行紧急电气清零。具体的叉管（ breech ）检测方法是保密的，并享有专利权。

为了保护其内容，机箱也会将内部操作屏蔽，使之不被射频信号探测

器检测到。

BIA 还有一种超保密的类型，其中叉管检测方法与一个能将多芯片模块和检测方法本身物理上加以摧毁的机构联系起来。

1.1.5. BIA 类型：无线型

除了使用一个外部天线而不是外部串口来送出一个广谱无线通信模块之外，无线型 BIA 硬件与标准型在结构上是相同的。

这种类型被设计成用于餐馆中，为了顾客的便利对交易进行授权。

在下面的说明中，需加到标准类型上的项目被标上了“+”号，而需从标准类型中减去的项目被标上了“-”号。

多芯片模块:

- 文件名称寄存器
- 共享对话密钥
- 专用对话密钥
- 消息密钥

部件:

- 串行口
+ 外部天线
+ 广谱无线串行模块（本领域公知）

1.1.6. BIA 硬件：ATM 型

ATM型BIA硬件是一个与重负载单纹扫描仪和一个串行口结合在一起的多芯片模块。各个部件被包围在一个防撞机箱中，机箱能提供防撞和对各部分进行射频屏蔽的功能。

该类型被设计成对 ATM 机的改型中。因此，扫描仪板是一个重负载传感器板，其总体结构中使用了 ATM 本身现有的屏幕和键盘。

在下面的说明中，需加到标准类型上的项目被标上了“+”号，而需从标准类型中减去的项目被标上了“-”号。

多芯片模块:

- 量值寄存器

- 文件名称寄存器
- 共享对话密钥
- 专用对话密钥
- 消息密钥

部件:

- 发光 PIC 键盘
- 2 行 40 列 LCD 屏

值得注意的是，由于 ATM 没有 LCD 屏或 PIC 键盘，在掩模 ROM 中无需设置这些设备的驱动程序。

1.1.7. BIA 硬件: 电话/有线电视型

电话/有线电视型 BIA 硬件是一个与单纹扫描仪和串行口结合在一起的多芯片模块。该模块在物理上附属于扫描仪上，整体上封装在塑料中，使要撞击它将会更困难。对于其中的部件，也能提供一定量的射频屏蔽。

这一类型被设计成与电话、电视远程控制器和传真机集成在一起。这样，就可以利用现有的键盘、 LCD 屏或电视屏幕来输入或显示数值。它还可以利用主终端的通信设备。比方说，传真机可以使用内置式传真调制解调器，电视远端可以使用 CATV 的电缆网络。

这种硬件（与其他类型相比）不够保密，原因是由于希望这些设备成本尽可能低，重量轻，与现有的低成本设备容易集成。

当然，具有更完整的机箱的、保密性能要好的类型也是可以实现的，而且应该是受到鼓励的。

在下面的说明中，需加到标准类型上的项目被标上了“+”号，而需从标准类型中减去的项目被标上了“-”号。

多芯片模块:

- 文件名称寄存器
- 共享对话密钥
- 专用对话密钥
- 消息密钥

部件:

- 发光PIC键盘
- 2行40列LCD屏

1.2. BIA软件

1.2.1. BIA软件命令接口

BIA的外部接口与一个标准调制解调器很相似，命令从一个控制终端使用外部串行线送来。当一个命令完成后，从BIA向该终端送出一个响应码。

每个BIA软件加载后都支持一组不同的操作。比方说，一个零售软件加载后只支持交易授权，而一个登记软件加载后支持个人识别和生物特征数据登记。

所有的BIA数据字段都呈可打印的ASCII码，字段之间由字段分隔符（或称“fs”）控制符隔开，记录之间通过新行分开。加密的字段是已使用基-64转换表（本领域内公知）转换成64位ASCII码的二进制码。

有些命令在有些结构中是没有的。例如，ATM BIA不能执行“Get PIC命令，因为没有PIC键盘与之相连。相反，ATM BIA支持“Set PIC命令。

响应码:

超时:

分配给该命令的时间已经期满。在LCD屏（如果有的话）上将显示出一个表示这一结果的消息。当某一给定命令的时间期满时，BIA工作起来就象取消按钮被按下一样。

取消:

“取消”按钮已被按下，整个操作被取消。这还具有一个清除所有已收集到的信息的副作用。在LCD屏（如果有的话）上将显示出一个表示这一结果的消息。

正常:

命令被成功执行。

其他:

每个命令都可能具有只对它有效的、具体的其他响应码。这些响应码通常具有伴随着代码的文字，并被显示在LCD屏上（如果有的话）。

消息:

它表示命令正在进行中，但是 BIA 希望以临时结果消息的形式向终端送出消息。这一结果也显示在 LCD 上（如果有的话）。这一功能被用于提示或状态消息。

命令:

在下面命令的变元表中，<>符括住的是独立的变元，[]符括住的是可选变元，| 符表示一个给定的变元可以是给出的多个选择之一。

设置语言<语言－名称>

该命令从编码到 BIA 内的多种不同的语言中选出一种，用于提示用户输入。

取得生物特征数据<时间>[主|副]

该命令请求 BIA 激活它的扫描仪，从个人取得生物特征消息输入，并存储到编码生物特征数据寄存器中。

首先，LCD 屏上将显示出“请将手指按到发光板上”的消息，并返回到终端。扫描仪板被照亮，提示用户输入他的生物特征数据。

<时间>值如为零则意味着对生物特征信息的扫描输入时间没有限制。

在扫描模式下，进行指纹扫描，并用一种指纹质量算法进行初始分析。如果扫描得不够好，BIA 还将进行新的扫描，直至<时间>中的秒数用完为至。当时间流逝、对指纹拍下快照进行分析时，有关指纹质量软件所检测到的问题的消息也被公布到 LCD 屏幕上，并送至终端。如果没有出现具有适当质量的指纹，BIA 返回一个超时误差码，并在 LCD 上显示出一个表示这一结果的消息。

一旦指纹质量算法肯定了指纹扫描的质量，指纹编码算法就将指纹的细节取出。只是随机选择细节的一个子集，但需保证足够多的供识别信息。接着，这些细节被随机地排序，并设置在编码生物特征数据寄存器中。然后，BIA 以成功结果代码进行响应。

如果[主|副]被指定（只可能出现在生物特征数据登记命令集中），那么选择的将是全部细节，而不仅仅是较小的子集。同样，主/副生物特征数据选择命令以把经编码的生物特征数据置入适当的寄存器结束。

无论操作成功与否，一旦扫描结束，指示扫描进程的灯将熄灭。

非常重要的一点是，相同的生物特征数据输入会产生不同的编码，这样会使任何试图找出捕获的 BIA 中的加密码的工作加难。这是由选择随机子集和对经编码的生物特征数据进行随机排序来实现的。

取得 PIC<时间>

该命令请求 BIA 通过读键盘来填充 PIC 寄存器。

首先，在 LCD 显示屏上将显示出“请输入你的 PIC，然后按<回车>键”，并送至终端，适当的键盘灯将点亮，键盘扫描即开始。

当<时间>项中指定的秒数用尽时，或者个人敲击“回车”键时，扫描即告结束。

需要注意的是，PIC 的各位数字在 LCD 屏上并不显示，而是对于每个具体类型的数字显示一个星号“*”，给用户一个反馈。当“修正”键被按下时，输入的最后一位数字被删除，从而允许用户修改输入错误。

PIC 输入结束时，键盘灯熄灭。

如果成功，该命令将返回正常码。

取得帐户索引代码<时间>

首先，在 LCD 显示屏上将显示出消息“现在请输入你的帐户索引码，然后按<回车>”，并送至终端。这将提示个人输入他的帐户索引码。当每个键被按下时，其值出现在 LCD 面板上。按下修正按钮可以清除这些值。当“回车”键被按下时，帐户索引码寄存器就将被置位。

在输入中适当键盘按键被点亮，当输入结束时，键盘灯熄灭。

如果成功，该命令将返回确认码。

取得职别索引代码<时间>

首先，在 LCD 显示屏上将显示出消息“现在请输入你的职别索引码，然后按<回车>”，并送至终端。这将提示用户输入他的职别索引码。当每个键被按下时，其值出现在 LCD 面板上。按下修正按钮可以清除其中的一个值。当“回车”键被按下时，职别索引码寄存器就将被置位。

在输入中适当键盘按键被点亮，当输入结束时，键盘灯熄灭。

如果成功，该命令将返回正常码。

确认量值<量值><时间>

确认证量值命令向终端送出一个消息“量值<量值>正确？”，并将其显示在LCD屏幕上。如果个人通过敲击“是（或回车）”键确认了该量值，量值寄存器被设置成该<量值>。这个<量值>必须是一个有效的数，不应带有控制符或空格等。在提示时，“是”、“否”和“清除”键将点亮。一旦提示结束，所有的灯光都将熄灭。

如果用户输入“否”，交易即被取消。

输入量值<时间>

该输入量值命令向终端发出“输入量值”的消息，并将它显示在LCD屏上。然后个人必须自己输入钱数。输入的每个字符都将显示在LCD屏幕上。所有适当的按钮都将被点亮。如果回车键被敲击，则量值寄存器被设置在从键盘输入的值上。一旦输入完成，所有的灯都将熄灭。

确认文件<名称><时间>

该确认文件命令向终端发出“文件<名称>正确？”的消息，并将它显示在LCD屏上。如果个人通过敲击“是（或回车）”键确认了文件，文件名称寄存器将被设置为<名称>。该<名称>必须是可打印的ASCII码，不能有控制符，而且前面和后面都不能带空格。在提示时，“是”、“否”和“清除”键将点亮。一旦提示结束，所有的灯光都将熄灭。

如果用户输入“否”，交易即被取消。

赋值寄存器<寄存器><文本>

该赋值寄存器命令将指定的通用寄存器<寄存器>设置成具有<文本>的值。该命令被用来设置商户代码、产品信息等。

取得消息密钥

该取得消息密钥命令使BIA产生一个56位的随机密钥，控制硬件将使用这一密钥对控制装置希望加到消息中的任何消息正文进行加密。BIA将以十六进制格式（本领域内公知的）返回产生的密钥。该消息密钥随即被加到生物特征数据－PIC块中。

格式消息<类型=标识|交易|帐户访问…>

格式消息命令指示BIA输出一个含有其收集的所有信息的消息。它还进行检查以确保所有的适合于那一特定消息<类型>的寄存器已经被设置。如果没有设置所有所需的寄存器，则BIA返回一个错误。该特定命令集软件将确定哪种消息能由BIA模式所形成，其他将被拒绝。

每一消息包括一个传输代码，该代码由BIA的唯一硬件标识代码和一个增量序列号组成。传输代码使DPC识别发送中的BIA和检测再提交袭击。

BIA使用BUKPT密钥管理系统从未来密钥表选择生物特征数据－PIC块加密56位DES密钥。而后，这一密钥用来利用密码块链接（CBC）对生物特征数据－PIC块加密。此外，也随机产生一个响应DES密钥，并被DPC用来对需加密的那部分响应进行加密。

注意：从生物特征数据－PIC块密钥分出响应密钥是非常重要的，因为每一加密密钥必须仅用在其自己的责任范围内。这样，如果有人想破译对专用代码编码的密钥，不会使生物特征数据－PIC公开。

该生物特征数据－PIC块由下列字段组成：

300字节授权生物特征数据

4－12位数字PIC

56位响应密钥

〔可选的56位消息密钥〕

注意，如果控制终端已经请求了用于一个消息的消息密钥，该消息密钥才出现。直到控制终端利用消息密钥对附于交易授权请求的任何消息体加密。

一旦完成所有的加密，BIA输出适当请求消息体（如交易授权请求消息），用消息鉴定代码（MAC）终结和保护。

利用BIA的保密112位DES MAC密钥计算出该MAC字段，并覆盖从第一个至最后一个的所有消息字段。MAC确保在该消息中无变化的DPC有效

地密封消息，同时仍然让控制终端检查明文字段。

当发出格式消息命令后，BIA 向终端发出消息“我正与 DPC 中心通话”，并将其显示于 LCD 屏上，表示根据请求正进行工作。

完成命令后，除了返回整个形成的消息之外，该命令返回正常。

表明响应<加密的响应> <时间>

表明响应命令指示 BIA 利用其当前的响应密钥，给来自系统的专用代码解密。

解密之后，出现一声钟鸣声，专用代码显示在 LCD 屏上持续<时间>秒。很快，该命令就将解密后的专用代码传送到控制终端。

确认专用<加密确认> <时间>

这一命令在安全网通信对话期间被终端采用，请求该个人确认来自外源的消息。该消息被加密并分为两部分：要求（challenge）和响应。

收到确认专用命令后，BIA 在 LCD 屏上显示要求消息文本为“正常<要求>？”，但不将其送到终端。当该个人确认要求后，BIA 利用专用对话密钥对响应加密，而后与正常响应代码一起返回到终端。如果该个人没有确认该要求，则 BIA 将“无效”响应代码以及“按你方请求已取消交易”返回，其也显示于 LCD 屏上。

注意，从未让该终端看见要求或响应的明文。

复位

复位命令指示 BIA 消除所有临时寄存器，LCD 屏、所有临时密钥寄存器，并关闭可能接通的所有键盘灯。

设置 PIC<值>

该命令给 BIA 的 PIC 寄存器赋值为<值>

注意，让一个不安全的装置提供 PIC 是一个潜在的安全问题，因为不安全的装置更容易受到窃听或替换。

设置帐户索引代码<值>

该命令将 BIA 的帐户索引代码寄存器赋值为<值>。

注意，让一个不安全的装置提供帐户索引代码是一个潜在的安全问题，因为不安全的装置更容易受到窃听或替换。

设置职别索引代码 M<值>

该命令给 BIA 的职别索引代码寄存器指定一个<值>。

注意，让一个不安全的装置提供职别索引代码是一个潜在的安全问题，因为不安全的装置更容易受到窃听或替换。

设置量值<值>

该命令给 BIA 的量值寄存器指定一个<值>

加密响应<加密响应消息>

该加密响应命令指示 BIA 利用其当前响应密钥对响应消息的加密部分进行解密。一旦被解密该响应返回到控制装置，例如用于显示在 ATM 终端的 LED 屏上。

注意，提供这一加密的能力是一个安全问题，一旦明文离开 BIA，该终端有能力随意处理它。

1.2.2. BIA 软件：支持库

BIA 软件由几个不同的软件库支持。其中的一些为标准的、通常可得到的库，但有些在 BIA 的内容方面有特殊要求。

1.2.2.1. 随机数发生器

由于 BIA 常常选择随机的 DES 密钥用于消息体和消息响应加密，所以所选择的密钥为不可预知的是很重要的。如果随机数发生器基于日时间、或基于一些其他外部可预知的机制，那么加密密钥将会很容易被碰巧知道该算法的对手猜出。为保证 BIA 所用加密技术的安全性，假定随机数发生器算法和加密算法均为公知的。

一个用于产生 DES 密钥的标准随机数算法在 ANSI X9.17，附录 C 中进行了定义（该领域公知）。

1.2.2.2. DSP 生物特征数据编码算法

该生物特征数据编码算法是一个用于确定通过人指尖上的纹理末端和分叉形成的细节的特有算法。一个完整的细节表存储于 DPC 中作为参考，当在对识别对象与已登记的个人进行比较时，该算法仅需要一部分表。

在生物特征数据登记以及识别期间，编码算法保证在结束生物特征输

入步骤之前发现足够的细节。

1.2.2.3 操作系统和设备驱动程序

BIA 是一个实时计算环境，要求实时嵌入操作系统使之运行。该操作系统负责处理来自设备的中断并对任务进行调度。

每一设备驱动程序负责操作系统和特定硬件之间的接口，如 PIC 键盘设备驱动程序或 CCD 扫描仪设备驱动程序。硬件是比如“PIC 键盘的键被压下”或“CCD 扫描器扫描完成”这样事件的来源。该设备驱动程序处理这些中断、中断事件，而后对事件采取行动。

1.2.2.4. DES 加密库

有一定数量的 DES 工具可公开得到。DES 工具利用 56 位的保密密钥提供从明文到密文的基于秘密密钥的加密，以及从密文到明文的解密。

1.2.2.5 公共密钥加密库

公共密钥加密支持库可从 Public Key Partners（其为业内已知的 RSA 公共密钥专利的持有人）处得到。公共密钥密码系统是非对称加密系统，其进行通信时无需秘密密钥的大量交换。为了使用公共密钥加密系统，用一个公共密钥对 DES 密钥加密，而后该 DES 密钥用来对一个消息加密。BIA 利用公共密钥密码系统提供秘密密钥的安全交换。

遗憾的是，公共密钥系统与秘密密钥系统相比没有很好地得到测试，因此在这种算法中，整体保密性较低。因此，本发明利用公共密钥密码用于通信安全性和短期留存的凭证交换，而不用于秘密的长期存储。终端用户个人和银行均用 DPC 识别，以建立网络凭证。网络凭证包括终端用户个人的标识以及连接的内容（即，TCP/IP 源和目标端口）。

1.2.2.6. DUKPT 密钥管理库

如果给出一个初始密钥和一个消息序列号，则用对每个交易导出的唯一密钥（DUKPT）管理库建立未来的 DES 密钥。未来密钥存储于未来密钥表中。一旦采用，从表中清除一个给定密钥。初始密钥仅用来产生初始未

来密钥表。因此BIA不存储初始密钥。

采用DUKPT建立一个密钥管理机构，其为每一个交易提供不同的DES密钥，而不遗留初始密钥的痕迹。这意味着即使成功捕获和分解给定未来密钥表，也不能泄露先前发送的消息，当传输信息的有效寿命为几十年时，这是一个重要目标。DUKPT在ANSI X9.24中作了详细规定（业内已知）。

最初研制DUKPT用于支持用于借方卡交易的PIC加密机构。在这一环境下，重要的是保护所有交易。假定罪犯记录了6个月期间的加密交易，而后从PIC键盘捕获并成功地提取加密代码。该罪犯而后可以对于在那6个月期间输送的每一消息制造一个新的伪造的借方卡。然而，在DUKPT的情况下，罪犯的盗窃和分解不会使他对先前的消息解密（尽管如果罪犯在分解后欲替换PIC键盘，新消息仍然可被解密）。

在生物特征－PIC情况下，罪犯甚至有一个艰苦的时期，即使消息被解密，将数字生物特征－PIC转换为实际的指纹要比将帐号－PIC转换到塑料卡困难得多，后者为无代价券系统的具大优点之一。

此外，如果罪犯能够解密，他可以解密，这使他将生物特征－PIC以电子方式提交给系统，以授权一个欺诈交易。尽管这是十分困难的，最好尽可能地限制罪犯可用的手段，因而利用DUKPT。

1.3.BIA软件命令集

1.3.1. BIA 软件：零售命令集

BIA/零售软件接口输出一个界面，使特定零售点销售终端与系统交互作用。

BIA/零售接口用来使该终端进行如下操作。

交易授权

为了进行这些操作，BIA/零售提供如下命令集：

设置语言<语言－名称>

取得生物特征数据<时间>

取得PIC<时间>

赋值寄存器<值>

取得帐户索引代码<时间>

确认量值<量> <时间>

输入量值<时间>

形成消息<类型>

示出响应<加密的响应> <时间>

复位

1.3.2. BIA 软件: CATV (集成远端) 命令集

BIA/CATV 软件接口输出一个命令集, 使终端与电话/CATV BIA 集成在一起, 与系统交互作用。支持下列操作。

远程交易授权

为进行这一操作, BIA/CATV 提供如下命令集:

取得生物特征数据<时间>

设置 PIC<文本>

赋值寄存器<寄存器> <文本>

设置帐户索引代码<文本>

形成消息<类型>

解密响应<加密的响应消息>

复位

1.3.3. BIA 软件: 集中 FAX 命令集

BIA/Fax 软件接口输出一个命令集, 使终端与传真 BIA 集成, 以与系统交互作用。支持下列操作:

安全传真提交

安全传真数据

安全传真跟踪

安全传真检索

安全传真拒绝

安全传真档案

安全传真合同接受

安全传真合同拒绝

电子文件档案检索

为进行这些操作， BIA/Fax 提供如下命令集:

取得生物特征数据<时间>

设置 PIC<文本>

设置职别索引代码<文本>

赋值寄存器<寄存器> <值>

取得消息密钥

形成消息<类型>

解密响应<加密的响应消息>

复位

1.3.4. BIA 软件: 登记命令集

BIA/Reg 软件接口输出一个界面，使通用计算机与系统交互作用以识别和登记个人。支持下列操作:

个人识别

生物特征数据登记

为支持这些操作， BIA/Reg 提供下列集令集:

设置语言<语言－名称>

取得生物特征数据<时间>〔主/辅〕

取得 PIC<时间>

赋值寄存器<寄存器> <文本>

取得消息密钥

形成消息<类型>

示出响应<加密的响应> <时间>

复位

1.3.5. BIA 软件: PC 命令集

BIA/PC 软件接口输出一个命令集，使通用计算机发送、接收或对电子文件签字、在网络中进行交易，并对网络上的站点提供生物特征数据导出的凭证。支持下列操作:

电子文件提交
电子文件数据
电子文件跟踪
电子文件检索
电子文件拒绝
电子文件档案
电子文件档案检索
电子签字提交
电子签字检查
远程交易授权
网络凭证
安全的连接
为支持这些操作， BIA/PC 提供下列命令集:
设置语言<语言－名称>
取得生物特征数据<时间>
取得 PIC <时间>
取得帐户索引代码<时间>
确认量值<量> <时间>
输入量值<时间>
确认文件<名称> <时间>
赋值寄存器<寄存器> <文本>
取得消息密钥
形成消息<类型>
示出响应<加密的响应> <时间>
确认专用<加密的确认> <时间>
复位

1.3.6. BIA 软件: 发行人命令集

BIA/ Iss 命令接口输出一个界面，使通用计算机与系统交互作用，以鉴定和提交批修改请求. 支持下列操作.

发行人批处理

为进行这一操作， BIA/Iss 提供如下命令集:

设置语言<语言－名称>

取得生物特征数据<时间> 〔主/辅〕

取得 PIC<时间>

赋值寄存器<寄存器> <值>

取得消息密钥

形成消息<类型>

示出响应<加密的响应> <时间>

复位

1.3.7. BIA 软件: 内部命令集

BIA/Int 输出一个命令集，使通用计算机与系统交互作用以识别个人。支持下列操作:

个人识别

为进行这一操作， BIA/Int 提供如下命令集:

设置语言<语言－名称>

取得生物特征数据<时间>

取得 PIC<时间>

赋值寄存器<寄存器> <值>

取得消息密钥

形成消息<类型>

示出响应<加密的响应> <时间>

复位

1.3.8. BIA 软件: ATM 命令集

BIA/ATM 软件接口输出一个命令集，使 ATM 对个人进行识别。支持下列操作:

帐户访问

为进行这一操作， BIA/ATM 提供如下命令集:

取得生物特征数据<时间>

设置 PIC<文本>

设置帐户索引代码<文本>

赋值寄存器<寄存器> <值>

形成消息<类型>

解密响应<加密的响应消息>

复位

1.4.终端

1.4.1.介绍

终端是一种控制 BIA 并经调制解调器、X.25 连接或国际互连网连接（业内公知的方法）连接到 DPC 的装置。终端有不同形状和尺寸，并需要不同版本的 BIA 进行其工作。任何向生物特征输入装置发出命令并从其接收结果的电子装置均可以是终端。

某些终端是运行在通用微型计算机上的应用程序，而其他终端是专用硬件和软件的结合。

尽管终端对于整个系统的功能是至关重要的，但是无论如何系统本身不能信任终端。无论终端向系统提供什么信息，系统总是以某种方式对其进行验证，或者通过向个人展示以便确认，或者通过其他先前登记的信息进行交叉核对。

虽然终端能读出 BIA 消息的某些部分，以便验证数据已经经过 BIA 进行了适当的处理，但是终端不能读出包括生物特征数据、PIC、加密密钥或帐户索引代码的生物特征识别信息。

特定 BIA 向终端输出某些安全功能，如 PIC 输入和专用代码显示。因此，这种装置比完全自包含的装置的安全性稍差，因而具有较低的安全度。

有许多不同终端类型，每一个被连接到一个特定形式的 BIA。下面将简述各个终端:

ATM（自动出纳机）

与 ATM 软件负载集成的 BIA/ATM 向 ATM 取款机提供生物特征 - PIC 访问。

BRT（生物特征登记终端）

连接于微机的加载有登记软件的标准 BIA 向银行提供将新个人登记到系统中的能力及其金融资产帐户和其他个人信息。

CET（验证的 Email 终端）

连接于微机的装有 PC 软件的标准 BIA 向个人提供发送、接收、存储、拒绝和跟踪经验证的 Email 消息的能力。

CPT（有线电视销售点终端）

连接于 CATV 宽带的装有 CATV 软件的 BIA/CATV 向具有生物特征－电视（TV）远端的个人提供对电视商场购物进行授权的能力。

CST（顾客服务终端）

连接于微机系统的装有内部软件的标准 BIA 授权雇员建立用于顾客服务目的的数据库请求。

EST（电子签字终端）

连接于微机的装有个人计算机软件的标准 BIA，向个人提供在文件上建立和验证电子签字的能力。

IPT（国际互联网销售点终端）

连接于微机的装有个人计算机软件的标准 BIA，通过国际互联网向个人提供从连到国际互联网的商户购买产品的能力。

IT（发行人终端）

连接于微机的装有发行人软件的标准 BIA 向银行提供对 DPC 的资产帐户的成批修改的能力。

ITT（国际互联网出纳终端）

连接于与国际互联网连接的微机的带有个人电脑软件的标准 BIA，向个人提供与他们喜爱的国际互联网银行进行交易的能力。

PPT（电话销售点终端）

与电话集成的装有 CATV 软件的 BIA/catv，向个人提供在电话中授权交易的能力。

RPT（零售销售点终端）

连接于 X25 网络或利用调制解调器的装有零售软件的标准 BIA，使个人在商店利用交易授权进行购物.

SFT（安全传真终端）

与传直机集成的装有传真软件的BIA/catv，向个人提供发送、接收、拒绝存档和跟踪安全传真消息的能力。

1.4.2.终端：零售销售点终端

1.4.2.1.目的

RPT的目的是使个人在商店购物时，不必使用现金、支票、借方卡或信用卡。

RPT使用BIA/零售对从个人到商户的金融交易进行授权。除了用来接收生物特征数据－PIC授权外，RPT提供标准借方以及信用卡扫描功能。

注意，此处仅对与生物特征数据相关的交易进行了详述。假设RPT也由标准信用和借方磁条卡读取器以及可选的智能卡读取器组成。

1.4.2.2.构造

每一RPT通过一个调制解调器、一个X.25网络连接、一个ISDN连接或类似机构连接到DPC。RPT也可以连接到其他装置，如电子收款机，从那儿可以得到交易量和商户代码。

RPT包括:

· BIA/零售
· 廉价微处理器
· 9.6kb调制解调器/X.25网络接口硬件
· 非易失RAM中的商户标识代码号
· 用于连接BIA的DTC串行口
· 磁条卡读取器（业内已知）
· ECR（电子收款机）接口
· 可选的智能卡读取器（业内已知）

1.4.2.3.标识

两个实体需要被识别，以便DPC积极地响应BIA交易授权请求：个人和商户

个人用生物特征数据－ PIC 识别，而商户用 DPC 识别，其交叉检查包含于 BIA 的 VAD 记录中的商户代码和被 RPT 加到交易请求中的商户代码。

1.4.2.4 操作

首先，商户将交易值输入其电子收款机。然后，个人输入其生物特征数据－ PIC、其帐户索引代码，而后确认其量值。然后 RPT 将产品信息和商户代码加到 BIA，指示 BIA 构造交易，而后将该交易经其网络连接（调制解调器，X.25 等）送到 DPC。

当 DPC 接收这一消息时，它确认生物特征数据－ PIC，用索引代码取得帐号，与登记的 BIA 的拥有者一起交叉检查该消息中的商户代码。如果一切都已检查完，DPC 形成并送出贷/借交易以进行交换。来自贷/借网络的响应加到专用代码以形成交易响应消息，而后 DPC 将其送回 RPT。RPT 检验该响应，看是否成功授权，然后向 BIA 送出响应，而后其显示个人的专有代码，终结交易。

1.4.2.5 安全性

由 BIA 的加密和 MAC 计算保证 RPT 和 DPC 间的消息的安全性。MAC 允许 RPT 查看消息的未加密部分，但 RPT 不能将其改变。加密防止了消息的加密部分向 RPT 公开。

每一零售 BIA 必须向商户登记。这有助于阻止 BIA 窃取。此外，由于 RPT 将商户代码加到每一消息，用不同的 BIA 代替商户的 BIA 受到在 DPC 进行的反复核查得以检测。

1.4.3. 终端：国际互联网销售点终端

1.4.3.1. 目的

国际互联网销售点终端（IPT）的目的是从计算机处的个人向商户对贷借金融交易进行授权，个人及商户均在国际互联网上。

注意，国际互联网简单地表示通用网，在该网中，商户、DPC 和 IPT 均能实时互联。因此，这一机构能同任何其他通用网一样工作:

1.4.3.2 构成

IPT 包括:

· BIA/PC

· 微机

· 国际互联网购物者软件应用程序

· 国际互联网（或其他网）连接

1.4.3.3 标识

除了识别个人外，IPT 也必须识别作为交易对方的远地商户。该商户也必须识别 DPC 和 IPT。

国际互联网购物者程序存储从其购物的商户的主机名（hostname）或其他形式的网名），以便验证商户的标识。由于商户将其所有合法的国际互联网主机名登记到 DPC 中，使得 DPC 交叉检查商户代码和哪一主机页名下存储的商户代码。

1.4.3.4 操作

首先，IPT 利用国际互联网与商户连接。一旦建立连接，IPT 通过产生并随后向商户发出对话密钥以保证这一连接的安全。为确保防止对话密钥公开，利用公共密钥加密法使用商户的公共密钥对其进行加密。当商户收到这一加密的对话密钥时，利用其专有密钥对其解密。这一过程称为通过公共密钥加密的秘密密钥交换确保连接的安全。

一旦连接，IPT 从商户下载商户代码以及价格和产品信息。一旦个人准备购买，他选择他希望购买的商品。然后，个人利用 BIA/PC 输入生物特征数据 - PIC，IPT 向 BIA 发送商户代码、产品标识信息和数量，指示它建立远程交易授权请求。而后 IPT 通过安全通道向商户发送该请求。

商户经与 IPT 同商户间的连接同类的安全连接与 DPC 连接，即利用公共密钥加密法发送一个安全对话密钥。然而，不同于 IPT - 商户连接，商户 - DPC 对话密钥对整天而不仅仅是一次连接有益。

商户连到 DPC，用对话密钥保证连接的安全，向 DPC 发送交易用于确认。DPC 确认生物特征数据 - PIC，交叉检查含在请求中的商户代码以及

在请求中发送的存在主机名下的商户代码，然后向贷/借网送一个交易。一旦贷/借网响应， DPC 建立一个应答消息，包括贷/借授权、加密的专用代码以及个人地址，并将消息送回商户。

一旦商户收到应答，它从应答中拷贝出个人的邮件地址，记录授权代码，并将应答消息送到 IPT 。

IPT 将应答交给 BIA， BIA 对专用代码解密并将其显示于 LCD 屏上，表示 DPC 识别出了该个人。 IPT 也示出交易结果是成功或失败。

1.4.3.5 安全性

由于系统一般假定网上的对手能在任意点破坏网络连接，各方在其实时交互作用时必须具有安全的通信。主要担心的不是信息的公开，而是消息的插入或更改地址。

整个公共密钥加密系统依靠的是具有用于公共密钥的可信源。这些可信源称为证实授权方，我们假设这样的源在不远的将来可在国际互联网上得到。

1.4.4.终端： 国际互联网出纳机终端

1.4.4.1.目的

国际互联网出纳机终端（ ITT ）用来识别个人以便进行国际互联网银行对话。 DPC 、银行计算机系统和个人均联到国际互联网。

有两个主要任务。第一个是提供从 ITT 至国际互联网银行的安全通信通道。第二个是向国际互联网银行提供无懈可击的身份凭证。一旦完成这两者， ITT 能提供安全的国际互联网银行对话。此外， BIA 的要求－响应验证能力用于对所有高值和/或不规则交易提供另外的安全性。

1.4.4.2.构成

ITT 包括:

· BIA （标准型 PC ）

· 微机

· 国际互联网出纳软件应用程序

· 国际互联网连接

IIT 利用连到作为个人国际互联网终端的微机的 BIA/PC 接收生物特征标识。

1.4.4.3.标识

个人和银行均由 DPC 识别以建立网络凭证。网络凭证包括个人标识以及连接的范围（即 TCP/IP 源和目的地端口）。

DPC 通过交叉检查银行送给 ITT 的代码和 ITT 送给 DPC 的银行主机名来识别银行。

1.4.4.4.操作

首先，ITT 连到国际互联网银行，确保银行具有用于处理个人的新对话所需的计算资源。如果银行具有足够的资源，它将银行标识代码送回 ITT。

一旦连接，ITT 指示 BIA 从个人获得生物特征数据－PIC 和帐户索引代码。而后 ITT 增加银行主机名及银行代码。使用所有这些信息，请求 BIA 形成网络凭证请求消息，ITT 经国际互联网将其送到 DPC。

当 DPC 收到这一消息时，它确认生物特征数据－PIC，用索引代码取得帐号，确保来自消息的银行代码与存储在远程商户数据库中的银行主机名下的银行代码匹配。DPC 还检查以保证以索引代码返回的帐号也属于该银行。如果所有检查完，DPC 用个人帐户标识、日时间和银行代码建立网络凭证。DPC 利用公共密钥加密和 DPC 的专用密钥签署这一凭证。DPC 检索银行的公共密钥、个人的专用密钥，并用凭证形成网络凭证响应消息。该响应消息用 BIA 响应密钥得以加密，而后送回 ITT。

当 ITT 收到响应时，它将该响应消息交给 BIA。BIA 解密，然后将个人专用代码显示于 LCD 屏上。银行的公共密钥存储于公共密钥寄存器中。由 BIA 产生两个随机对话密钥。第一个密钥，称为共享对话密钥，以明文向 ITT 披露。ITT 利用这一共享对话密钥确保与银行连接的安全。

其他对话密钥，称为专用对话密钥，不与 ITT 共享。它用于 BIA 的要求－响应机制，该机制让银行直接从个人得到非常规交易的特定确认，无需涉及（不值得信任的）ITT。

在收到共享对话密钥后，ITT请求BIA形成安全连接请求消息，其包括对话密钥和网络凭证，所有均用银行的公共密钥得以加密。然后IIT将安全连接请求消息送回银行。

当银行收到请求消息时，它利用其自己的专用密钥对该消息解密。而后，它用DPC的公共密钥对实际的网络凭证解密。如果网络凭证有效，且没过期（若干分钟后，凭证时间过期），则对个人授权，对话继续，对话密钥用来确保安全。

无论何时个人进行任何非常规或高值交易，银行会希望请求个人确认那些交易格外安全。为此，银行向ITT发送用专用对话密钥加密的要求－响应消息，ITT将该要求－响应消息发送到BIA。BIA对消息解密，显示要求（通常用的形式：将2031.23美元转给Rick Adams，可以？），当个人通过击“可以”钮确认时，BIA用专用对话密钥对响应再加密，并将那一消息送到ITT，ITT将其传到银行，确认交易。

1.4.4.5.安全性

该系统利用公共密钥加密法提供凭证并保证ITT和银行之间的通信安全。

为使这一机构正常起作用，银行必须知道DPC的公共密钥，并且DPC必须知道银行的公共密钥。双方保证各自公共密钥安全，避受未授权的修改，对系统的安全性来说是很重要的。注意，任何人均可读到公共密钥但不能修改。当然，任何对话或秘密密钥必须保密，免于发现。在对话结束后，必须消毁那些秘密密钥。

对非常规交易的额外确认步骤是必要的，因为由于病毒、骇客和个人疏忽，要保证个人计算机应用的安全相对困难。银行应该可能地将可用于IIT的常规资金汇兑限制到仅包括向充分了解的机关（如公益公司、主要信用卡发卡行等）的资金汇兑。

1.4.5.终端：电子签字

1.4.5.1.目的

电子签字终端（EST）被个人利用，以生成用于电子文件的不能被伪

造的电子签字。 EST 允许个人签署电子文件或验证已经存在于这种文件上的电子签字。

1.4.5.2. 构成

EST 包括:

. —BIA/PC;

. —微机;

. —消息分类 编码算法;

. —调制解调器, —X.25 连接, 或—国际互联网连接;

. —电子签字软件应用程序。

EST 使用一个连到由电子签字软件应用程序控制的微机的 BIA/PC。

1.4.5.3. 识别

为了创建一个不需使用公共/专用密钥令牌, 需要做三件事。首先, 要签字的文件需要唯一地被标识, 需要记录当天的时间, 需要识别进行签字的个人。这就连接了文件, 个人和时间, 创建一个唯一的时间盖印的电子签字。

1.4.5.4. 操作

首先, 要签字的文件由一个产生消息分类编码的一消息分类编码算法处理。这样一个算法是业界公知熟知 RSA 的 MD5 算法。根据其特性, 特定地设计消息分类算法, 使得不可能接近另一个产生同一消息分类编码的文件。

然后, 使用 BIA, 个人输入他的生物特征数据 - PIC, 向 BIA 传送消息摘要代码, 加入文件的名称, 所得的数字签字请求消息被送至 DPC, 用以授权和储存。

当 DPC 接收到该请求时, 它进行生物特征数据身份检验, 一旦个人被核实, 它收集消息摘要代码, 个人的生物特征数据帐号, 日时间, 文件名称以及收集签字的 BIA 的标别, 并将它们存储到电子签字数据库 (ESD)。然后, 该 DPC 构成一个由 ESD 记录号、日期、时间和签字者姓名组成的一签字代码正文串。并与个人的专用代码一起将该签字代码送回 EST。

为检查一电子签字，通过MD5算法（业界公知）发送该文件，并且所得的值以及电子签字代码与请求个人的生物特征数据－ PIC 一起送至BIA，该消息被送至DPC。该DPC检查每一签字用于验证，并在合适时作出响应。

1.4.5.5.安全

BIA对与电子签字有关的任何数据不进行加密，从而与特定的MD5值一起以明文发送文件标题。这种情况适用于签字验证。

这样，尽管签字不能被伪造，但一些细节（包括文件名称）易于被截取。

1.4.6.终端：验证的电子邮件终端

1.4.6.1.目的

验证的电子邮件终端（ CET ）的目的是提供给个人一种向系统中的其他个人传送电子消息的方式，同时用于识别发送方，并且验证接收和接收方，并保证消息传送的保密性。

CET使用一BIA/PC以识别发送方和接收方。通过加密该消息以建立安全性。然后在上载期间使用发送方的BIA加密消息密钥，并在下载期间使用接收方的BIA解密该消息密钥。

1.4.6.2. 构成

发送方和接收方CET均包括:

. 一BIA;

. 一微机;

. 一调制解调器，一X.25连接，或一国际互联网连接;

. 接收电子邮件的能力

.一验证的电子邮件应用程序。

CET 通常是一个带有电子邮件应用程序和网络连接的一个微机，它使BIA产生一生物特征数据－ PIC授权，以发送和接收验证的电子邮件。

1.4.6.3. 识别

为了保证消息的传送，必须识别发送方和接收方。

当发送方将该消息上载到 DPC 时，他使用他的生物特征数据－ PIC 识别他自己。发送方希望向其发送文件的每个接收方或者通过生物特征数据帐户识别号得以识别，或者通过传真号及扩展得以识别。为了使一接收方下载该消息，他使用他的生物特征数据－ PIC 识别他自己。该过程类似于个人至个人的电话呼叫。

1.4.6.4. 操作

个人上载一文件或消息并使用他的生物特征数据－ PIC 识别他自己以起动消息的传送。然后个人验证该文件的名称，并且加密该电子邮件消息并上载。

一旦上载一消息，发送方接收一消息识别代码，该代码用于请求至每一接收方的文件的当前的传递状态。

DPC 向每一接收方发送一电子邮件消息，通知他们何时到达一验证消息。

一旦接收方接收到该通知，接收方可根据其意愿，通过提交他的生物特征数据－ PIC 和通过 DPC 对其确认，选择接受或拒绝该消息或一组消息。

一旦成功地传输至所有接收方，在一预定时期之后，通常为 24 小时，删除该文件。希望归档该文件的个人，与传送消息的所有个人的指示一起，在删除该消息之前可以提交消息归档请求。

1.4.6.5. 安全性

为了保证传输的安全性，该文件在路由中被保护以免被公开。 CET 通过使用 BIA 产生的 56 位消息密钥以实现这一点。作为生物特征数据－ PIC 的一部分，由于 BIA 负责加密该消息密钥，加密密钥被安全地发送至 DPC 。

当个人下载该消息时，与专用代码一起发送加密的消息密钥，以允许接收方对该消息进行解密。注意，由于接收方都接收同一消息，最好所有的接收方具有这一消息密钥。

对于 ITT ，由于一旦个人确认了该文件名称，一个修改的 CET 可发送

任何它所希望的文件，所以个人必须注意保护他们的 CET 应用软件不被暗中修改。

1.4.7.终端：安全传真终端

1.4.7.1.目的

安全传真终端（ SFT ）的目的是给个人提供一种将传真消息传送给系统中的其他个人而同时提供发送方的标识，接收和接收方的验证，及保证消息传送的保密性。

每个 SFT 使用一个集成的 BIA/catv 以识别发送方和接收方，通过加密完成通信的安全性。

1.4.7.2.构成

发送方和接收方 SFT 均包括：

. — BIA/CATV

. —传真机

. 可选 ISDN 调制解调器

SFT 是一个通过调制解调器连接到 DPC 的一个传真机。系统对传真象对另一种类型的已经验证的电子邮件一样进行处理。

1.4.7.3. 识别

对于安全传真，有几不同的安全级，但在绝大多数的安全版本中，要验证发送方和所有接收方的身份。

发送方发送其消息到 DPC 时，他使用其生物特征数据－ PIC 和职别索引代码识别他自己。为了收取这传真，每个被列出的接收方再次使用生物特征数据－ PIC 和职别索引代码识别其自己。

另外，用电话号码识别该接收站点。该电话号码登记至 DPC 中。对于安全保密传真，每个接收方用电话号码和其扩展进行识别。

1.4.7.4.操作

有五种基本类型的可由 SFT 发送的传真

I. 非安全传真

非安全传真相当于标准的传真。发送方输入接收站点的电话号码并发送该传真。这种情况下，不识别发送方，且传真发送至给定的电话号码以希望该传真传送至正确的接收方。 SFT 将所有这种非安全性的传真的顶行标记为“非安全”。从非 SFT 传真机接收到的所有传真总是被标记为非安全的。

II. 安全发送方传真

在安全发送方传真中，发送方选择传真机上的“安全发送方”方式，输入其生物特征数据－ PIC 及他们的职别索引代码。然后传真机连接至 DPC 并发送生物特征数据－ PIC 信息。一旦 DPC 验证个人的身份，该个人通过将文件送入传真扫描器发送该传真。这种情况下，传真实际被发送至数字地存储该传真的 DPC 。一旦所有的传真都到达该 DPC ，该 DPC 开始发送该传真至每一目的地，与在每一页的顶部用“发送方安全”、姓名、职别和发送方公司标记每一页。

III. 安全传真

在安全传真中，发送方在传真机上选择“安全的”方式，输入他们的生物特征数据－ PIC 及他们的职别索引代码，并输入接收方的电话号码。一旦系统验证发送方的身份和每个接收方电话号码，然后个人通过将该文件送入传真扫描器发送该传真。该传真然后发送到以数字方式存储该传真的 DPC 。一旦整个传真到达 DPC ，该 DPC 向目的地发送一小的首页，指示悬置的安全传真，发送方职别和身份以及等待的页数并且和跟踪代码。该跟踪代码被自动地输入至接收方的传真机的存储器中。

为了检索该传真，接收方公司的雇员可以在他的传真机上选择“检索传真”按钮。通过使用跟踪代码选择要检索的悬置 传真，然后输入生物特征数据－ PIC 。如果不是想要的传真，用户可以按下“拒绝传真”按钮。尽管为了这样做，他还必须向系统标识他自己。一旦是一个有效的公司成员，则该传真被下载至接收方的 传真机上。与发送方的身份和职别信息一起，在每页的顶部标记有“安全”。

IV. 安全保密传真

在安全保密传真中，发送方在传真机上选择“安全保密”方式，输入

他们的生物特征数据－ PIC 及他们的职别和索引代码，并输入每一接收方的电话号码和系统扩展。一旦 DPC 验证发送方的身份和每个接收方电话号码及扩展，然后个人通过将该文件送入传真扫描器发送该传真。该传真发送至数字地存储该传真的 DPC 。一旦整个传真到达该 DPC，该 DPC 向每一目的地发送一小的首页，指示悬置安全保密传真、发送方职别和身份、接收方职别和身份、以及等待的页数并且和跟踪代码。该跟踪代码被自动地输入至接收方的传真机的存储器中。然而能检索该传真的个人仅是其扩展代码被指示的个人。

该个人选择“检索传真”按钮，选择要检索的悬置传真，然后输入他的生物特征数据-PIC 。一旦是一个有效的接收方，则该传真被下载至接收方的传真机上。与发送方的职别和身份信息一起，在每页的顶部标记有“安全保密”。

V. 安全保密合同传真

就向接收方实际传送该传真而言，除了该传真被标为“合同 而非安全保密之外，该传真的处理与安全保密传真一样。另外， DPC 自动地归档合同传真。通过 SFT 接收该合同传真之后，任何接收方可以接收或拒绝该合同。根据选择， DPC 完成电子公证人的角色。

发送至系统然后被传送至接收方的任何传真可以发送给任何数量的接收方而不须停止该发送传真机。另外，任何所发送传真的跟踪号码被输入至传真机的存储器，通过选择“状态”按纽并选择特定传真悬置跟踪代码在发送机上可以生成关于任何发出传真的状态报告。 DPC 发出一个立即发送至发送传真机的详细描述用于每一接收方发送状态的报告。

使用任何安全的或安全保密的传真，对于发送方或对于接收方之一存在一种选择以归档该传真(以及该传真的发送方和接收方)用于将来参考。为此在成功传送之后任何安全传真被保留一定时间(例如 24 小时)。不管何时请求一档案，归档跟踪代码返回该个人。该归档代码用于检索传真和用该系统归档的传真状态报告.

一定时间（例如 24 小时）之后，归案的传真放置在只读辅助存储器中。检索一归档的传真需要人工干预，可能需要多至 24 小时。

1.4.7.5. 安全性

该 SFT 系统努力工作以保证发送方身份的接收，它同样向发送方确保接收方实际确认对该文件的接收。

为了保护发送方和接收方之间的通信免于被截取，传真终端使用 BIA 提供的消息密钥装置加密该传真。由于 BIA 将消息密钥加密为生物特征数据－ PIC 的一部分，所以加密密钥安全地发送至 DPC 。

当个人接收到任何类型的一安全传真时，与专用代码一起发送加密的消息密钥，以允许接收方解密该消息。注意由于他们都接收相同的消息，最好所有的接收方都具有该消息密钥。

1.4.7.6. 注意

发送安全传真与发送电子邮件非常相似，并同用同一软件的大部分。

可能构造不具有集成BIA/传真设备但有一部分适于连有一外部BIA/pc和适用于使用 BIA 的软件的传真终端。

1.4.8. 终端: 生物特征数据登记终端

1.4.8.1. 目的

生物特征数据登记终端（ BRT ）的目的是登记新的个人，包括他们的生物特征数据－ PIC ，邮件地址，专用代码，电子邮件地址，职别列表和用于发送和接收电子消息和传真的职别索引代码，金融资产帐户的列表和可以访问的帐户索引代码，所有的都使用他们的生物特征数据－ PIC 。

登记处理的目标是从可靠机构的位置处的个人得到个人信息，其中该信息可被确认。这包括但不限于零售银行业务分支机构和企业人员部门。每个参与可靠机构具有由一群雇员使用的一个 BRT 。上述雇员被授权执行登记，每个雇员对于登记的每个人负责。

1.4.8.2. 构成

一个微机和屏幕，键盘，鼠标

一个 BIA/登记

9.6kb 调制解调器/X.25 网络连接（在业界公知）

一个生物特征数据登记软件应用程序

BRT 使用一个所连的 BIA/登记用于生物特征数据输入，并通过一 9.6kb 调制解调器或一 X.25 网络连接（在业界公知）与该系统相连。生物特征数据登记终端位于这样一个位置，他们在物理上是安全的，例如零售银行业务分支机构。

1.4.8.3. 识别

为了响应 BIA/登记的登记请求，对于 DPC 需要识别 3 个实体：登记雇员，机构和 BIA/登记。该雇员必须已经被授权为那个机构登记个人。

用 BRT 取得的机构代码通过交叉检查 BIA 的拥有者来识别机构和 BIA。通过在开始登记应用程序时输入他的生物特征数据－ PIC，雇员向系统村识他自己。

在系统上登记个人之前，机构使用他的标准客户识别过程（签字卡，雇员记录，个人信息，等等）。由于允许登记个人按照他们的意愿将资金从那些帐户转帐，和/或使用公司的名称发送电子消息，所以尽可能认真地验证个人身份对于机构是很重要的。

1.4.8.4. 操作

在登记期间，个人输入主要和辅助生物特征数据。个人必须使用食指。如果个人失去了食指，可以使用下面一个最里面的手指。要求使用特定手指允许现有的欺诈检查工作。

鼓励个人选择一个主要和辅助手指，在 DPC 身份检查期间最好给出主要手指，使得个人应当拿出最常使用的手指作为主要的。当然，如果必要，DPC 可以根据操作选择以改变主要和辅助生物特征数据的设计。

作为生物特征数据编码处理的一部分，BIA/R 确定个人是否已经输入“一个好的指纹”。注意有一些人其工作引起意外删除他们的指纹，例如用研磨剂或酸工作的那些人。不幸的是这些个人不能使用该系统。在这一阶段，他们被监测并被通知他们不能参与。

在系统中央数据库所提供的一系列 PIC 中，个人选择一个 4 到 12 位数

字的 PIC 。然而，该 PIC 必须由系统确认。这牵涉到两次检查：其一，使用同一 PIC 的其他个人的号码不能太大（由于 PIC 用于减少由生物特征数据比较算法检查的个人的数目），其二，就生物特征数据而言，登记的个人不能与在同一 PIC 组中的其他个人距离太“近”。如果出现上述情况，拒绝登记并且向 BRT 返回错误消息，并通知个人请求不同的 PIC 。该系统可选择地返回具有一个“相同匹配”错误条件，该条件指示在那个 PIC 下，个人已经在该系统中有一个记录。

PIC 为零（ 0 ）允许系统分配一个 PIC 至个人。

个人构造一个包括单词或短语的保密专用代码。如果个人不希望构造一个将由终端随机地构造一个专用代码。

个人还可以安排他们的金融资产代码列表。该列表描述了哪个帐户索引代码指向哪个帐号（例如： 1 表示借， 2 表示贷， 3 表示紧急借等等）。注意仅在登记机构是银行并且帐户为特定银行机构所拥有时上述情况才会发生。

即使在每次登记后，在完成先前欺诈检查时之前，使用系统个人不能进行利用系统的操作。这通常需要几分钟，但是在高负载期间，它需要几个小时。仅当系统没有发现先前欺诈时，才启动个人帐户。

1.4.8.5. 安全性

如果发现个人即使欺诈该系统一次，该 DPC 也对该罪犯进行一次数据库内广泛的偶然生物特征数据数据库搜索。每夜执行这些的一部分，通过在轻负载活动状态期间进行耗时处理，使得系统所要寻找的特定个人被从该数据库中分离出。

执行登记操作的雇员，仅当初始启动该登记系统时，通过使用生物特征数据－ PIC 标识他们自己。这对雇员很方便，但是由于未在场的或“临时借出的” BRT 可能是欺诈的根源，对系统的来说可能有安全性问题。

1.4.9. 终端：客户服务

1.4.9.1. 目的

客户服务终端（ CST ）的目的是提供至系统数据库的各方面的内部 DPC 支

持的个人访问。支持人员需要回答使用系统时了现问题的个人、发行人、机构的商户提出的咨询。

1.4.9.2. 构成

CST 包括:

. 一微机

. 一 BIA/Int

. 以太网/令牌环/FDDI 网络接口

. 数据库检查和修改应用程序

通过诸如令牌环、以太网、光纤（ FDDI ）等的一个高速局域网连接，每一个 CST 被连接至该系统。每一 CST 能询问每一数据库并显示这些询问的结果。然而， CST 仅显示基于单个终端用户的特权的字段和记录。例如，一个标准的客户服务雇员不能看到对于一给定 BIA 的 VDB 记录的加密代码，尽管他们能看到哪个商户或个人当前拥有那个 BIA 。

1.4.9.3. 识别

对于 CST 允许访问该数据库，该系统必须识别个人和 BIA 。另外，必须确定个人的特权等级，使得可对访问进行适当的限制。

1.4.9.4. 操作

通过输入他们的生物特征数据 - PIC 提供识别，使用一 CST 的个人开始一对话。 BIA 构造一识别请求消息并将其发送至 DPC 用以验证。一旦系统验证个人，尽管受个人先前所分配的 DPC 特权等级的限制，该 CST 应用程序正常操作。

1.4.9.5. 安全性

为了安全的目的， 经过一预定空闲时间后， DPC 终止至 CST 应用程序的连接。

不能以任何方式修改数据库应用程序是很重要的，不管是故意的或是通过病毒引入的。为此，个人 CST 不拥有任何软盘驱动器或其他的可拆卸介质。还有，可执行的数据库应用程序的读访问被严格地限制到需要知道的那些人。

为了保护CST和数据库之间的通信免于暗中修改或公开，CST加密CST和数据库之间的所有通信。为此，CST产生一对话密钥，该密钥在向系统登录对话期间发送至服务器。该对话密钥用于加密和解密在此期间发生的与DPC有关的所有通信。

尽管假设安全通信和非修改数据库应用程序，DPC保证操作CST的个人不能访问的DPC数据字段不被发送至CST的数据库应用程序。同样，任何时间任何个人不能访问或被允许修改个人的生物特征数据信息。

DPC和支持中心可以位于一处，或者由于围绕CST其本身相当高的安全性，支持中心本身可被分开。

1.4.10. 终端：发行人终端

1.4.10.1. 目的

发行人终端的目的在于允许在发行银行的雇员以安全和可识别的方式向DPC提供成批资产帐户修改操作。

1.4.10.2. 构成

IT包括：

. 一微机

. 一调制解调器，X.25网络或至该系统的国际互联网连接.

. 一BIA/Iss

. 至银行内部网络的网络连接

发行人终端使用一发行人BIA以授权大量的金融资产信息的增加和删除。

1.4.10.3. 识别

在这种操作中，必须识别银行，必须识别正确授权的银行雇员，还必须识别其资产帐户被增加或删除的所有的个人。

银行用于识别那些希望将他们在该银行的帐户加至他们的资产帐户列表中的个人。如在生物特征数据登记中，银行通过使用签字卡和个人信息完成该工作。通过交叉检查IT所提交的发行人代码和登记在BIA/Iss的VAD记录中的发行人代码，DPC识别该银行。使用生物特征数据－PIC以识别实际提交该批处

理的银行雇员。

1.4.10.4. 操作

为了加入一金融资产帐户，个人将其生物特征数据识别号码与要加入的帐户一起提供给银行（在最初的生物特征数据登记步骤中识别号码被提供给个人）。在正确地识别人个之后，将该识别代码和帐户列表传送给 IT，以用于后面的向系统的批处理提交。

不管何时银行认为合适，银行中授权的个人通知 IT 向 DPC 上载成批的帐户增加/删除。为了这样，授权的个人输入其生物特征数据－ PIC， IT 加入对话密钥，加上银行的发行人代码，并且以此 BIA/Iss 构造一发行人批处理请求消息，随后 IT 将该消息传送至 DPC。 IT 使用消息代码加密该批处理，然后发送它们。

当系统接收到该发行人批处理请求时，它确认该 BIA 是一 BIA/Iss，该 BIA/Iss 登记至发行人代码所要求的银行，并且在生物特征数据－ PIC 内识别的个人被允许向该 DPC 提交用于该银行的批处理请求。如果这样， DPC 处理所有的请求，按要求跟踪错误。一旦完成，与包括在处理期间发生的任何错误的加密批处理一起， DPC 返回个人的专用代码。

1.4.10.5. 安全性

该交易的安全对于系统的安全性而言很重要。意欲欺诈的罪犯仅需发现一种方法将其他人的帐户加到他的生物特征数据识别代码，然后可以根据意愿进行欺诈。最终罪犯被抓住，且从数据库中删除，但随后其他人的帐户被罪犯侵袭。

加密保证银行和 DPC 之间的传输不被截取，从而帐号在传送时受到保护。

交叉检查银行和 BIA/Iss 意味着 IT 和 BIA 必须妥协地向 DPC 提交假的增加/删除消息。这样，银行保证 IT 是物理上安全的，并且仅有授权的个人被允许使用它。

要求个人提交批处理保证负责人员“循规蹈矩”，该负责人员的工作是在该批处理的建设和传输中确保遵循合适的银行安全措施。

1.4.11. 终端: 自动柜员机

1.4.11.1. 目的

生物特征数据 ATM 的目的在于允许个人存取现金和进行其他 ATM 业务而不使用一银行间卡。通过提供一生物特征数据－ PIC 和一帐户索引代码并检索一银行帐号而完成。对于系统的用户，这取代了银行间卡（业界已知）＋ PIC 机制，作为一种识别帐户和授权个人的方法。假设 ATM 将继续接受银行间卡。

1.4.11.2. 构成

IT 包括:

. 一标准的 ATM

. 一集成的 BIA/ATM（仅有扫描器）

. 一至 DPC 的连接

生物特征数据 ATM 使用一集成的 BIA/ATM 以识别个人并允许他们使用生物特征数据－ PIC 和一帐户索引访问金融资产。在 ATM 中安装一 BIA/ATM，使用 ATM 的当前 PIC 键盘以便输入 PIC 和帐户索引代码。使用 X.25 或调制解调器，将该 ATM 连接至系统。

这样构造 BIA/ATM 使得它以最简单的方式与现存的 ATM 网络进行集成在一起。使得在安全性和集成的难易之间达成妥协。

1.4.11.3. 识别

为了正确地响应一 BIA/ATM 帐户请求，对于 DPC 需要识别三种实体: 个人、银行和 BIA/ATM。

通过交叉检查 ATM 存储的银行代码和 BIA/ATM 的银行代码，识别银行。在 VAD 中成功地定位 BIA/ATM 以识别 BIA/ATM，并且通过标准生物特征数据－ PIC 识别个人。

1.4.11.4. 操作

为了使用 ATM，个人向 BIA 输入他们的生物特征数据－ PIC 和帐户索引代码。BIA 形成一帐户访问请求消息，通过 ATM 该消息随后被发送至 DPC。DPC 确认生物特征数据－ PIC 以及紧急帐户索引代码，并与专用代码一起将所得的

资产帐号送回 ATM.

ATM 要求 BIA 解密该响应，并在 ATM 的显示屏上显示该专用代码。 ATM 还检查该响应以发现个人是否执行一标准的帐户访问，或“强制”帐户访问。如果指示为一强制的帐户访问， ATM 可能提供一有关个人可用数量的假的或误导信息，这种行为的具体情况将随着 ATM 的不同而改变。然而，当进行强制交易时， ATM 将不向个人提供任何指示。

1.4.11.5. 安全性

通过 BIA 的加密和 MAC 计算， ATM 和 DPC 间的消息被保护。 MAC 意味着 ATM 不能不经检测而改变消息的内容，并且加密防止公开消息的加密部分。

由于 BIA/ATM 没有 LCD 或 PIC 键盘，它要求 ATM 提供所有的文本提示并收集个人的所有输入。这种情况的安全性次于 BIA 执行操作的情况，但是由于通常 ATM 很坚固，它可以被称为 wash 。

1.4.11.6. 注意

当个人指示他正在执行强制下的交易时，在银行和个人之间确定 ATM 的行为。特定的银行可以选择限制访问，或改变余额信息，或显示假屏幕。假屏幕是这样一种数据显示，该数据被预先确定为不正确的，使得强制方不能非法地获取关于个人金融资产的准确数据。在这种情况下定义 ATM 的准确行为超出了本发明的范围。

1.4.12. 终端: 电话销售点终端

1.4.12.1. 目的

电话销售点终端（ PPT ）的目的是对使用特制电话从商户购买商品的个人发出的借贷金融交易进行授权。

1.4.12.2. 构成

PPT 包括:

. —BIA/catv

. 快速连接的数字调制解调器（见 Voice View 专利（业界公知））

. —电话（键盘，耳机，话筒）

. —微机

. — DSP （数字信号处理器）

. —标准电话线

该 PPT 使用与无绳电话、蜂窝电话或标准电话相连和集成在一起的一 BIA/catv，接受生物特征数据标识。

1.4.12.3.识别

为了使 DPC 授权一个交易，必须识别个人和商户。

为了识别个人，使用生物特征数据－ PIC 标识。

为了识别电话定购商户，商户和人个要呼叫的商户的所有电话号码要登记至 DPC。这样，当个人提交一授权时，他还提交他要呼叫的电话号码，该电话号码用商户的列出的电话号码进行交叉检查。

1.4.12.4. 操作

个人呼叫通过纸件商品目录、报纸、杂志或其他基本打印媒体机制销售其商品的商户。PPT 使用一个共享电话语音线路的特定调制解调器与商户交换数字信息。

在个人决定购物一情形下，每当个人进行一次电话呼叫时，PPT 即跟踪用户所输入的电话号码。使用 DSP 以检测拨号音、振铃、连接等等，以告诉实际输入的电话号码，以区别于扩展信息（分机）或电话消息系统的导航等。

一旦呼叫商户，该商户的销售人员就将所有的相关信息（包括产品、价格和商户代码）数字地下载至 PPT。注意在操作时，调制解调器中断扬声器。

当产品信息被下载时，PPT 提示个人关于生物特征数据－ PIC、帐户索引代码并请求个人确认该购买数量。然后加上电话号码和商户代码并加密该消息。使用快速连接调制解调器将授权信息发送至商户。

当商户接收到授权信息时，商户验证价格和产品信息，并通过使用国际互联网或其他一些通用网络的安全的通信信道将该次交易传送至 DPC。使用公共密钥加密和一秘密密钥交换保证至 DPC 的连接。

接收到并解密电话授权时，DPC 检查电话号码及商户代码，确认该生物特

征数据－ PIC 并发送该次交易至用于授权的借/贷网络。如果授权成功， DPC 将购物者的地址加到响应消息上并发送该响应至商户。

商户从DPC 接收该响应，复制邮件地址并使用一快速连接调制解调器通过简单对话再次传送该消息至个人。完成至 IPT 的传输时，响起和谐的乐声，断开调制解调器并在 LCD 屏幕上显示个人的专用代码（由 BIA 解密）。商户的销售代表确认个人的邮件地址是有效的。如果这样，中断呼叫并完成该次交易。

1.4.12.5. 安全性

关于电话交易安全性的一个方面是电话系统本身的安全性。除了生物特征数据标识外，主要问题是保证个人呼叫的号码确实到达所要求的商户。

注意 PPT 和商户之间的通信线路是不安全的，所以来自个人的至商户的购物授权可能被截取。然而，由此不会产生任何金融利益，因此认为这不重要。

由于在分清 PIC 输入和专用代码解密以及展示的责任中的固有问题， PPT 由于价格和重量所需的安全性相对较低。

1.4.13. 终端: 有线电视销售点

1.4.13.1 目的:

有线电视（ CATV ）销售点终端（ CPT ）的目的是对从电视（或“ TV ”）机前的个人到在电视上展示销售对象的商户的贷方或借方金融交易进行授权。

1.4.13.2 构造

CPT 包括:

· 一个 BIA/catv

· 一个具有集成的 BIA/catv 的电视遥控器

· 一个有线电视数字信号解码器

· 一个有线电视遥控器读取器

· 一个幕上显示机构

· 对有线电视宽带双向通信信道的访问装置

CPT 使用与电视的远程控制设备集成在一起的 BIA/catv 来接受生物特

征数据标识。该远程控制设备与一个电视机顶盒通信，该机顶盒本身与宽带有线电视网通信。该终端包括：与 BIA 通信的电视远程控制逻辑装置，以及与有线宽带网通信的电视机顶盒。

1.4.13.3 识别

在该交易中，该商户与个人必须都被识别以进行交易。

该个人通过生物特征数据－ PIC 识别。

该商户通过一个商户凭证来识别；该凭证在该产品显示在电视上时由 CATV 广播员创建。每个产品广播具有一个商户－产品凭证，该凭证包括一个商户代码、一个时间、一个期限和一个价格，它标记有公共密钥加密和 CATV 网广播员的私人密钥。这个商户－产品凭证仅能由网络广播员生成。

1.4.13.4 操作

当电视广播、商业信息（ infomercial ）、或家庭购物频道显示一个产品时，有线电视网也同时广播描述简短说明，价格以及商户－产品凭证的数字信息。该数字信息被 CPT 处理并暂时存储，随时可以被用户在作出购买决定时访问。

为购买当前被显示的某种东西，该个人选择专用电视远端的幕上显示功能，它指示 CPT 在屏幕上显示关于当前看到的产品的本文信息。

首先通过幕上显示向个人提示他希望购买的产品数量。然后他被提示输入他的生物特征数据－ PIC，以及他的帐户索引码。一旦他核实了最终购买价格是可以的，则该产品、价格、商户、代码、商户－产品凭证、以及频道号连同生物特征数据－ PIC 被用于构成一个远程交易授权请求消息。该请求通过有线电视宽带双向通信信道传送到该商户用于授权。

请注意每一个希望以这种方式销售产品的商户必须具备采用宽带有线电视网接收定货信息的能力。

接到该授权请求后，该商户利用一个加密的互联网连接或一个 X.25 连接将该请求提交给 DPC 。

如果 DPC 授权了该交易，它可以构成一个授权响应，该响应除了包括授权代码和加密的专用代码之外还包括该个人的当前邮件地址。一旦该商

户收到授权，他将授权以及邮件地址拷贝，然后将授权发送回CPT， CPT向该个人显示专用代码，结束该交易。

1.4.13.5 安全

该系统结构不允许罪犯重放从有线电视宽带网截获的消息，但他们能够阅读该消息中的一些部分。如果不希望这样，那么该消息可以通过采用一个任选的有线电视中心公共密钥，或有线电视机机顶盒（在行业中已知的）与有线电视本地局之间的“链路级”加密进行加密。

为了保证商户与DPC之间的连接的安全，该连接采用一个每天都改变的对话密钥，它已先前被使用一个公共密钥加密密钥更换系统而更换。

1.5 系统描述：数据处理中心

1.5.1 介绍

数据处理中心（ DPC ）以处理金融交易授权和个人登记作为其主要职责。另外， DPC为保密传真、电子文件，以及电子签字提供存储和检索。

每一个DPC站点由通过如在DPC概观图（数字**）中所示的LAN（在该行业中已知的）连接在一起的几台计算和几个数据库构成。面对在任意单个DPC站点出现的故障或严重的硬件故障，多个相同的DPC站点保证了可靠的服务。而且，每个DPC站点具有后备电源并在其所有的关键硬件及数据库系统中具有多个冗余。

DPC部件分成三类：硬件、软件和数据库。以下是每种部件逐类的简短说明。更详细的说明出现于后面的章节中。

1.5.1.1.硬件

FW 防火墙机器： DPC站点的进入点。

GM 网关机器：系统协调器和消息处理器。

DPCLAN DPC局域网：连接DPC站点。

1.5.1.2.数据库

IBD 个人生物特征数据库：从个人的生物特征数据以及PIC码识别个

人。

PFD 先前欺诈数据库：列出曾欺诈过该系统的个人并检查一个生物特征数据是否与这些个人任何之一匹配。

VAD 有效设备数据库：存储需用于证实和解密 BIA 消息的信息。

AOD 设备拥有者数据库：存储关于 BIA 拥有者的信息。

ID 发行人数据库：识别参与该系统的发行银行。

AID 被授权个人数据库：存储被允许使用个人或发行人 BIA 设备的个人的列表。

RMD 远程商户数据库：存储处理与电话和有线电视商户的交易所需的信息。

EDD 电子文件数据库：存储用于被授权的个人检索的电子文件，比如传真以及电子邮件。

ESD 电子签字数据库：存储用于被一个第三方用户识别的电子签字。

1.5.1.3 软件

MPM 消息处理模块：通过与需用于执行消息任务的其他软件模块和数据库进行协调而进行每个消息的处理。

SNM 序列号模块：进行 DUKPT 序列号处理。

MACM 消息授权代码模块：进行 MAC 的验证和生成。

MDM 消息解密模块：进行 BIA 请求和响应的加密和解密。

PGL PIC 组列表：利用 PIC 以及依赖于 PIC 组的列表的数据库元素结构管理对 PIC 组的查找。

IML IBD 机器列表：进行主和后备数据库机器的查找，这些数据库机器专用于保存对每个给定 PIC 组的 IBD 记录。

1.5.1.4 术语

当定义数据库模式时，以下术语被用于描述字段类型：

int<x> 使用<x>字节存储器的整型

char<x> <x>字节的字符数组

text 可变长度字符数组

<type><x> 长度为<x>的指定类型数组

time 用于存储时间和日期的类型

biometric 用于存储生物特征数据的二进制数据类型

fax 用于存储传真图象的二进制数据类型

当描述数据库存储要求时，术语“预期”意味着全加载的系统的预期条件。

1.5.2 协议说明

终端通过向 DPC 站点发送请求包来完成它们的任务。该 DPC 站点发送回一个包含有关于该请求的成功或失败的状态的应答包。

通信是通过一个逻辑的或物理的面向连接的消息传送机制比如 X.25 连接、TCP/IP 连接或电话呼叫到达一个调制解调器库。每个对话在 DPC 向终端送回响应之前保持到终端连接的开放。

该请求包包含一个 BIA 消息部分和一个终端消息部分:

BIA 消息部分

协议版本号

消息类型

4 字节 BIA 标识

4 字节序列号

<消息专用数据>

消息鉴别码（MAC）

终端消息部分

<终端专用数据>

该 BIA 消息部分是由一个 BIA 设备建成。它包括一个或两个生物特征数据，一个 PIC，授权数量，以及由该终端设置的通用寄存器的内容。注意：该 BIA 消息部分中的 MAC 只适用于该 BIA 部分而不适用于终端部分。

一个终端可以将用于请求消息的另外的数据放在该终端消息部分中。BIA 提供一个消息密钥以允许该终端保密终端部分数据。当需要时，BIA 自动将消息密钥加入包的加密的生物特征数据－PIC 块。然而，该终端自己进行消息密钥的加密。

应答包包含一个标准首部和两个任选的自由格式消息部分：一个有一个 MAC 而另一个没有。

标准首部

协议版本号

消息类型

任选的带有 MAC 的自由格式消息部分

<消息专用数据>

MAC

任选的没有 MAC 的自由格式消息部分

<另外的消息专用数据>

带有 MAC 的消息部分被传送到 BIA 使得它可以确认应答的这一部分没有被窜改，然后显示该个人的专用代码。没有 MAC 的消息部分被用于发送大量的数据，如传真图象，这些数据不被传送到 BIA 用于 MAC 确认，因为 BIA 到终端的连接可能是有限带宽的。

1.5.3. 处理包

在本发明的一个具有多个 DPC 站点的实施例中，一个终端只需将它的请求传送到这些 DPC 站点中的一个，一般是最近的一个，因为只要需要，该站点通过运行分布式交易而自动地更新其他站点。

当 DPC 的防火墙机器中的一个收到一个包时，它将该包发送到 GM 机器之一用于实际处理。每个 GM 具有一个消息处理模块，它进行用于处理请求的 DPC 部件之间的协调并将应答传回到发送方。

1.5.4. 确认以及解密包

DPC 收到的所有包，除了那些不是由 BIA 建成的，都包含一个 BIA 硬件识别码（该包的 BIA 标识），一个序列号，和一个消息鉴别码（MAC）。GM 要求 MAC 模块确认包的 MAC 然后通过序列号模块检查序列号。如果两个检查都通过，GM 将该包传送到消息解密模块用于解密。如果任何一个检查失败，则 GM 记录一个警告，终止对该包的处理，并向 BIA 设备返回一个错误消息。

目前，不是由BIA建成的仅有消息类型是保密传真数据请求和电子文件数据请求。

1.5.5.应答包

DPC收到的每一个包可以包含一个存储在该包的加密的生物特征数据－PIC块中的任选的应答密钥。在DPC应答一个含有一个应答密钥的请求之前，它用该应答密钥加密应答包。它也生成一个消息鉴别码并将其附加在包上。

加密应答包的唯一例外应用于错误消息。错误从来不被加密并从不包含机密信息。然而，大多数应答包含有一个指示请求成功与否的状态码或应答码。例如，当DPC拒绝一个贷方授权时，它不返回一个错误包，而是返回一个标准交易应答包，该包带有一个被设置成“失败”的应答码。

1.5.6.DPC过程

DPC具有两个在处理请求时共同使用的过程。

1.5.6.1.个人识别过程

对于要求DPC识别个人的请求，DPC执行以下过程：利用PIC码，DPC检索IBD机器列表查找主和后备IBD机器，该机器负责处理对给定PIC码的识别。然后，DPC根据谁被加载最少而将识别请求发送到主机器或后备机器。IBD机器以该个人的IBD记录或一个“个人未找到”错误做出应答。

IBD机器检索给定PIC的所有IBD记录。利用一个专有生物特征数据硬件设备，IBD机器将每个记录的主生物特征数据与该个人的生物特征数据比较，得到一个指示两个生物特征数据之间相似性的比较分数。如果任何一个生物特征数据都不具有一个足够接近的比较分数，则采用辅生物特征数据重复比较。如果任何一个辅生物特征数据不具有一个足够接近的比较分数，则IBD机器返回一个“个人未找到”错误。否则，IBD机器返回该个人的完全IBD记录，从中可以获得诸如专用代码、帐号、职别等这样的字段。

1.5.6.2. 紧急应答过程:

对于包含一个帐户索引的请求， DPC 处理个人选择他或她的紧急帐户索引的情况。处理该请求的 GM 立即通知 DPC 客户支持人员，记录一个警告，并且如果应答包具有一个应答码，将该码置位成“紧急”。发出请求的 BIA 设备的拥有者的责任是等待“紧急”应答码，并提供进一步的帮助，比如在 ATM 终端章节中描述的假屏幕机构。无论何时访问紧急帐户索引， DPC 也增加该个人的 IBD 记录的紧急使用计数。

1.5.7. 协议请求

下面的章节描述每个协议请求/应答以及 DPC 为实现它们而采取的动作。

协议包的列表是:

- 个人识别
- 交易授权
- 登记
- 帐户访问
- 发行人批处理
- 保密传真发送
- 保密传真数据
- 保密传真跟踪
- 保密传真检索
- 保密传真拒绝
- 保密传真档案
- 保密传真合同接受
- 保密传真合同拒绝
- 保密传真机构变化
- 电子文件发送
- 电子文件数据
- 电子文件跟踪
- 电子文件检索

· 电子文件拒绝
· 电子文件档案
· 电子文件档案检索
· 电子签字
· 电子签字验证
· 网络凭证

1.5.7.1. 个人识别

个人识别请求

BIA 部分:

4 字节 BIA 标识

4 字节序列号

加密（ DUKPT 密钥）的生物特征数据 - PIC 块:

300 字节授权生物特征数据

4 - 12 位数字 PIC

56 位应答密钥

MAC

终端部分: （未使用）

个人识别应答

加密（应答密钥）的:

专用代码文本

个人名字

生物特征数据识别码

MAC

个人识别请求包含一个生物特征数据 - PIC 块， DPC 利用该块通过个人识别过程来识别该个人。如果该个人被识别，则 DPC 以该个人的名字、生物特征数据标识以及专用代码做出应答。否则， DPC 以一个“未知个人”错误做出应答。

1.5.7.2. 交易授权

交易授权请求

BIA 部分:

4 字节 BIA 标识

4 字节序列号

加密（ BUKPT 密钥）的生物特征数据 PIC 块:

300 字节授权生物特征数据

4 - 12 位数字 PIC

56 - 位响应密钥

〔可选 56 位消息密钥〕

帐户索引

价格

标识

〔可选自由格式产品信息〕

〔可选商户代码（电话号码，通道号码 + 时间，主名）〕

〔可选发送地址请求〕

MAC

终端部分: （未使用）

交易授权响应

加密（响应密钥）的:

专用代码内容

授权响应

授权细目（授权代码、交易标识等）

〔可选个人地址信息〕

响应代码（失败，正常，紧急）

MAC

有两种基本的交易授权子类型: 零售和远程销售:

对于零售授权， DPC 利用请求的生物特征数据 PIC 块识别购物个人。如果该人不能被识别出， DPC 以“未知个人”错应答之。

之后， DPC 根据涉及的资产帐户类型（如 Visa™, or American Express™）将一个外部授权请求（将 BIA 装置拥有者的资产帐户记入贷方

并将个人的资产帐户记入借方）发送给业已存在的几个金融授权服务机构中的一个。如果该外部金融授权服务机构批准了该交易，则 DPC 将该外部授权码以及一个“正常”应答码送回该 BIA 装置。否则，DPC 将否认授权的原因送回并将应答码置为“失败”。在任何一种情况下，DPC 在响应中包括该个人的专用代码。

当 DPC 利用请求的帐户索引查寻个人的资产帐户时，被选择的帐户可以是“紧急”帐户。如果发生这种情况，DPC 则进行紧急响应过程。然而，外部授权仍会发生。

远程授权可用电话、邮件订货或有线电视商户产生。DPC 以处理零售授权相同的方式处理远程授权但存在以下例外情况:

i) 远程授权包含一个远程商户码，DPC 对照远程商户数据库检查该远程商户码以便证实该包的商户标识是否与数据库中存储的标识相匹配。此外，被记入贷方的资产帐户是远程商户的帐户，而不是 BIA 装置拥有者的帐户。

ii) 另外，产生远程授权的 BIA 装置倾向为个人 BIA 装置。DPC 对照被允许使用 BIA 装置的个人的授权个人数据库列表检查被识别的个人的生物特征数据标识。如果该个人不被授权使用该装置，则 DPC 拒绝该授权请求。

iii) 最后，授权包可以包含一个“发送地址”指示器。该指示器告之 DPC 包括在响应包中的个人地址并反被用于邮件订货购物。

1.5.7.3 登记

登记请求

BIA 部分:

4 字节 BIA 标识

4 字节序列号

加密（DUKPT 密钥）的生物特征数据 - PIC 块:

1000 字节主生物特征数据

1000 字节辅生物特征数据

4 - 12 位数字 PIC

56 位响应密钥

56 位消息密钥

MAC

终端部分:

加密（消息密钥）的:

姓名

地址

邮区号

专用代码

资产帐户列表（帐户索引码，帐号）

紧急帐户（帐户索引码，帐号）

职别列表（职别索引码，职别名）

登记响应

状态代码

加密（响应密钥）的:

专用代码内容

PIC

生物特征数据识别码

DPC 被选择的 PICs 的列表（如果拒绝原始 PIC 选择的话）

状态代码（正常，拒绝）

MAC

个人通过一个生物特征数据登记终端（ BRT ）向 DPC 进行登记。该 BRT 向 DPC 发送一个含有主、辅生物特征数据及个人识别代码的登记包，以及辅助数据，诸如个人姓名、地址、金融资产帐户列表、专用代码以及紧急帐户。可选择的是，该个人可以含有电子邮件地址、包括职别和职别索引码在内的职别列表以及社会安全号（即“ SSN ”）。个人可以选择她或他自己的 PIC 代码或者允许系统选择之。在修改步骤任何以前输入过的数均可被修改或删除。

在任何时刻，为了实施方便起见，仅有一个 DPC 站用作为登记站。由

各非登记 DPC 站收到的登记请求包被送到当前登记站。该登记 DPC 站完成全部登记检查，将 IBD 记录赋予 IBD 机器，并完成更新所有其他 DPC 站所需的分配的交易。

登记 DPC 站选择用于那些不规定一个登记请求的诸登记请求的 PIC 代码，将 IBD 记录存储在主和备份 IBD 机器上（如 PIC 组列表中所规定的那样），并且在运行分配的交易以便更新其他 DPC 站之前检查登记包的 PIC 和生物特征数据适当性。

DPC 运行一个个人识别代码和生物特征数据样品复制检查步骤，其中在登记步骤中得到的生物特征数据和个人识别代码被相对于当前与相同的个人识别代码相关的所有以前登记的生物特征数据进行检查。DPC 会因下列原因拒绝该登记：该 PIC 码太一般了，或者此生物特征数据太类似于在所选的 PIC 之下存储的其他生物特征数据了。为帮助个人选择一个可接受的 PIC，DPC 产生一个 PIC 码的短列表，为此该登记将会被保证其将保留一段时间。BRT 然后向该个人提示一个新的可从好的 PIC 列表选择出的 PIC。

1.5.7.4 帐户访问

帐户访问请求

BIA 部分:

4 字节 BIA 标识

4 字节序列号

加密（BUKPT 密钥）的生物特征数据 PIC 块:

300 字节授权生物特征数据

4 - 12 位数据 PIC

56 位响应密钥

〔可选 56 位消息密钥〕

帐户索引

MAC

终端部分:（未使用）

帐户访问响应

加密（响应密钥）的:

专用代码内容

〔可选 PIL〕

资产帐户号码

响应码（失败，正常，紧急）

MAC

帐户访问请求允许配有 BIA 的出纳机为个人提供一个使 ATM 识别自己的更为安全、更为方便的方式。

GM 利用包的生物特征数据－ PIC 识别个人并使用规定的帐户索引选择哪个资产帐户号码以便检索。

当 GM 使用请求的帐户索引查寻该个人的资产帐户时，被选择的帐户可以是“紧急”帐户。如果这种情况发生，GM 则执行紧急响应过程。

1.5.7.5 发行人批处理

发行人批处理请求

BIA 部分:

4 字节 BIA 标识

4 字节序列号

加密（BUKPT 密钥）的生物特征数据－ PIC 块:

300 字节授权生物特征数据

4 － 12 位数字 PIC

56 位响应密钥

56 位消息密钥

发行人代码

MAC

终端部分:

加密（信息密钥）的批处理列表:

加<生物特征数据 Id> <帐户索引> <资产帐户>

〔<紧急标志>〕

去除<生物特征数据 Id> <帐户索引> <资产帐户>

发行人批处理响应:

加密（响应密钥）的:

专用代码内容

应答码（失败，正常，紧急）

MAC

加密（消息密钥）的失败列表:

失败<命令> <代码>

...

发行人批处理请求允许发行银行或其他机关在个人生物特征数据库上执行例行的维护。如果DPC从非发行人BIA装置收到发行人批处理请求，DPC将记录一个安全侵犯警告，并且DPC也拒绝处理该请求。

DPC识别通过下列个人识别过程识别提交批处理请求的个人。DPC然后检验该个人被登记入授权的个人数据库中以便使用发送发行人终端中放入的BIA装置。

DPC还使用请求中的发行人代码去查寻发行人数据库中的设备拥有者标识，并将其与有效设备数据库中存储的设备拥有者标识相比较以确保该发行人代码不是伪造的。

DPC然后执行消息密钥的加密批处理列表中的加和删命令。该批处理列表是一种新行分开的命令列表。

有效命令是:

加<生物特征数据Id> <帐户索引> <资产帐户> [<紧急标志>]

去除<生物特征数据Id> <帐户索引> <资产帐户>

加命令将资产帐户加入在规定帐户索引中的帐户列表。可选的紧急标志指明该特定的帐户索引是否被对待成个人紧急帐户。如果帐户列表中现存的资产帐户不属于该发行人，则命令失败。这种特性避免了一个银行未经个人察觉或授权从另一个银行的客户中加入或去除资产帐户。

去除命令清除帐户列表中的存储在规定帐户索引中的个人资产帐户。如果当前帐户列表中所存储的资产帐户与发行人欲去除的帐户不符，则命令失败。

对于每一个不能正确执行的批处理中的命令，GM记入一个安全侵犯警告并先将一个登记项附加给失败的响应列表。失败的登记项包括命令的内容和错误代码。

1.5.7.6 安全传真传递

安全传真传递请求

BIA 部分:

4 字节 BIA 标识

4 字节序列号

加密（ DUKPT 密钥）人生物特征数据 - PIC 块:

300 字节授权生物特征数据

4 - 12 位数字 PIC

56 位响应密钥

56 位消息密钥

安全代码（不安全的，发送方安全的，安全的，安全 - 保密）

发送方职别索引代码

发送方传真号

发送方传真扩展信息

接受方列表

〔可选档案传真指示器〕

〔可选合同/协议指示器〕

终端部分:（未使用）

安全传真提交响应

加密（响应密钥）的:

专用代码内容

传真跟踪号

MAC

当 DPC 接收到一个安全传真提交请求时，其通过执行个人识别过程从请求的生物特征数据 - PIC 中识别该个人。这一识别，连同职别索引代码描述的个人职别被提供给接受方，使得传真的发送方总被可靠地识别。

DPC 产生一个用于跟踪目的的跟踪号码并将该号码、发送方生物特征数据标识，安全模式以及消息密钥存入一个新建的 EDD 文件记录。对于接受方列表中的每一个接受方，DPC 还建立一个接受方记录。DPC 然后等待发送传真机发送利用消息密钥加密的传真数据。

如果请求包含一个“档案传真”或“合同/协议”指示器，EDD 在档案数据库中放置一个文件和接收方记录的复制件。对这些记录的任何后续更新也都对规档的版本进行。

传真数据以分开的步骤发送使得如果发送方在输入其生物特征数据和 PIC 中产生错误，系统将在他将文件送入传真机而浪费时间之前通知他。

1.5.7.7.安全传真数据

安全传真数据请求

BIA 部分：（未使用）

终端部分:

传真跟踪号码

加密（消息密钥）的:

传真图像数据

安全传真数据响应

状态（未完成，正常）

安全传真数据请求允许一个安全传真机向 DPC 发送传真图象以便提供给业已规定的接受方。这一请求不涉及任何生物特征数据标识，却依赖于保密消息密钥以便安全地发送图象。

传真图象数据由安全传真提交请求登记的消息密钥加密。一但 DPC 已经收到完整的传真，它便向每一个接受方传真号码发送一个安全传真到达通知消息。DPC 通过对 EDD 查询所有含传真跟踪号码的接受方记录检索接受方列表。接受方记录包含目的地传真号码和可选扩展部分。发出到达通知之后，DPC 将每一个接受方记录传递状态字段更新为“已通知”。注：如果目的地传真号码占线，DPC 将传递状态字段标记为“占线”并周期性地重新发送该通知（即每 10 分钟一次）直到成功并在此时将该状态字段更

新为“已通知”。

到达通知如下:

安全传真到达通知（传真信息）

发送方姓名，公司，职别以及传真号码

传真跟踪号码

关于如何卸下传真的指令。

在所有接受方或者收取传真或者拒绝传真之后，DPC 通过传真仅向发送方发送一个状态通知。发送方可以使用安全传真跟踪请求（参见下述内容）询问 DPC 以便得到所有接受方的当前状态。

状态通知如下:

安全传真状态通知（传真信息）

发送方姓名，公司，职别以及传真号码

传真跟踪号码

接受方列表表明:

姓名，公司，职别以及传真号码

发送日期和状态

合同/协议状态

DPC 在 EDD 机构表中寻找每个个人的公司和职别信息。

对于那些未登记入系统中从而不能接收安全传真的个人，或对于那些非接受方安全模式，DPC 不向他们发送安全传真到达通知，而是向他们直接发送传真。如果传真线占线，DPC 每隔 10 分钟试一次直至成功发送传真为止。

1.5.7.8 安全传真跟踪

安全传真跟踪请求

BIA 部分:

4 字节 BIA 标识

4 字节序列号

加密（DUKPT 密钥）的生物特征数据 - PIC 块:

300 字节授权生物特征数据

4 - 12 位数字 PIC

56 位响应密钥

56 位消息密钥

传真跟踪号码

MAC

终端部分: （未使用）

安全传真跟踪响应

加密（响应密钥）的:

专用代码内容

用于跟踪响应传真图象的消息摘要

状态代码（正常，失败）

MAC

用于接受方状态列表的传真图象

DPC 通过检查针对传真的所有的 EDD 接受方记录并产生一个显示记录的传真消息来处理安全传真跟踪请求。如果作出跟踪请求的个人不是传真文件的发送方，则 DPC 将状态码置为失败并在响应中放入空传真。

跟踪响应传真包括用于描述对于每个接收方所发送的传真的状态的信息。该传真包括如下状态信息: 线路忙，传真到达通知已发送，传真已发送，传真被拒绝，合同被接受等等。

跟踪通知如下:

安全传真跟踪通知（传真消息）

发送方名称，公司，职别及传真号码

传真跟踪号码

接收方显示列表:

名称，公司，职别及传真号码

发送日期及状态

合同状态

1.5.7.9. 安全传真检索

安全传真检索请求

BIA 部分:

4 字节 BIA 标识;

4 字节序列码

加密的（ DUKPT 密钥）生物特征数据 - PIC 块:

300 字节授权生物特征数据

4 - 12 位数字 PIC

56 位响应密钥

传真跟踪码

MAC

终端部分: （未使用）

安全传真检索响应

加密的（响应密钥）:

个人代码

56 位消息密钥

状态（未完成，正常，无效接收方）

传真图像的消息摘要

MAC

加密的（消息密钥）:

传真图像

DPC 通过执行个人识别程序，利用生物特征 - PIC 来识别提出检索请求的个人。若不存在关于该个人及具体的传真的 EDD 接收方记录，则 DPC 应答“无效接收方”状态信息。

DPC 根据其返回给请求方的正确传真跟踪号码和生物特征标识符，从 EDD 文件记录中检索加密的传真图像。

传真图像包括一个显示传真是否是合同/协议、发送方名称、公司、职别、传真号码及扩展信息的首页。

当最后一个接收方接收或拒绝传真后，DPC 通过传真（参见上面的安全传真数据）将状态通知发送给传真的发送方。然后，在一个可配置的时间段内进行调度，将文档和接收方记录从 EDD 中删除。该时间段使得接收方有足够的时间去判断是否将传真存档。

1.5.7.10. 安全传真拒绝

安全传真拒绝请求

BIA 部分:

4 字节 BIA 标识

4 字节序列号

加密的（ DUKPT 密钥）生物特征 - PIC 块:

300 字节的授权生物特征

4 - 12 位数字 PIC

56 位响应密钥

传真跟踪码

MAC

终端部分: （未使用）

安全传真拒绝响应

加密的（响应密钥）:

个人代码

状态代码（正常，无效接收方）

MAC

DPC 利用生物特征 - PIC 来识别提出安全传真拒绝请求的个人。DPC 找到以请求的传真跟踪号码和个人的生物特征标识为关键字的 EDD 接收方记录。若不能找到记录，则请求以“无效接收方”状态而宣告失败。

当最后一个接收方接收或拒绝传真后，DPC 利用传真（见上面的安全传真数据）将状态通知发送给传真的发送方，然后进行调度，在一个可配置的时间段内将传真和跟踪记录从 EDD 中删除。该时间段使得接收方有足够的时间去判断是否将传真存档。

1.5.7.11. 安全传真存档

安全传真存档请求

BIA 部分:

4 字节 BIA 标识

4 字节序列号

加密的（ DUKPT 密钥）生物特征 - PIC 块:

300 字节授权生物特征

4 - 12 位数字 PIC

56 位响应密钥

传真跟踪号码

MAC

终端部分: （未使用）

安全传真存档响应

加密的（响应密钥）:

个人代码

状态代码（正常，无效个人）

MAC

DPC 使用生物特征 - PIC 来识别提出安全传真存档请求的个人。DPC 找到以请求的传真跟踪号码和个人的生物特征标识符为关键字的 EDD 接收方记录。若不能找到记录并且该个人不是发送方或者不是接收方之一，则请求以“无效个人”状态而宣告失败。否则，DPC 将文件和接收方记录复制进 EDD 文档数据库。其后对这些记录的任何改变也将被复制进存档版本。

1.5.7.12. 安全传真合同接受

安全传真合同接受请求

BIA 部分:

4 字节 BIA 标识符

4 字节序列号

加密的（ DUKPT 密钥）生物特征 - PIC 块:

300 字节授权生物特征

4 - 12 位数字 PIC

56 位响应密钥

传真跟踪号码

MAC

终端部分: （未使用）

安全传真合同接受响应

加密的（响应密钥）：

个人代码

状态代码（正常，无效接收方）

MAC

DPC使用生物特征－PIC来识别提出合同接受请求的个人。DPC找到以请求的传真跟踪号码和个人的生物特征标识为关键字的EDD接收方记录。若不能找到记录，则请求以“无效个人”状态而宣告失败。否则DPC将接收方记录的合同状态字段更新为“已接收”并且为传真的发送方生成一个状态通知（见上面的传真数据）。

1.5.7.13.安全传真合同拒绝

安全传真合同拒绝请求

BIA部分:

4字节BIA标识符

4字节序列码

加密的（DUKPT密钥）生物特征－PIC块:

300字节授权生物特征

4－12位数字PIC

56位响应密钥

传真跟踪号码

MAC

终端部分:（未使用）

安全传真合同拒绝响应

加密的（响应密钥）：

个人代码

状态代码（正常，无效个人）

MAC

DPC使用生物特征－PIC来识别提出合同拒绝请求的个人。DPC找到以请求的传真跟踪号码和个人的生物特征标识为关键字的EDD接收方记录。

若不能找到记录则请求以“无效接收方”状态而宣告失败。否则，DPC 将接收方记录的合同状态字段更新为“拒绝”并且为传真的发送方生成一个状态通知（见上面的传真数据）。

1.5.7.14. 安全传真机构变更

安全传真机构变更（安全传真消息）

发送方名称，公司，职别及传真号码

机构变更列表。

机构变更通过一个安全传真消息提交给 DPC。由客户的技术支持工程师来进行传真消息中所请求的变更，并验证提交请求的个人被允许为该具体的公司登记个人。由于传真是安全传真，因此发送方的身份及其职别均已被确认。

1.5.7.15. 电子文件提交

电子文件提交请求

BIA 部分:

4 字节 BIA 标识符

4 字节序列码

加密的（DUKPT 密钥）生物特征 - PIC 块:

300 字节授权生物特征

4 - 12 位数字 PIC

56 位响应密钥

56 位消息密钥

接收方列表

MAC

终端部分: （未使用）

电子文件提交响应

加密的（响应密钥）:

个人代码文本

跟踪号码:

状态代码（正常，无效接收方）

MAC

当 DPC 接收到一个电子文件提交请求后，通过执行个人识别过程来识别个人。

接着 DPC 生成一条 EDD 文件记录并为其分配一个唯一跟踪号码。DPC 将记录的发送方标识代码初始化为所识别出的个人的生物特征标识代码，将消息密钥初始化为请求中的消息密钥。

接着 DPC 查找个人生物特征数据库中的每一个接收方并为其生成一条 EDD 接收方记录。用跟踪号码，接收方生物特征标识代码，及“未完成”传送状态来初始化每条记录。若一个接收方也找不到，则 DPC 应答出“无效接收方”状态。

1.5.7.16. 电子文件数据

电子文件数据请求

BIA 部分：（未使用）

终端部分：

跟踪号码

命令（异常中止或数据）

〔可选的消息偏移量〕

完成指示

加密的（消息密钥）：

消息正文

电子文件数据响应

状态（未完成，正常）

电子文件数据请求允许个人将文件正文（一个或多个部分）发送给 EDD 以向接收方传送。该请求不涉及任何生物特征标识，而是根据秘密的消息密钥来秘密地发送文件正文。

假设请求正文是由存储在 EDD 文件记录中的消息密钥来加密的并附加在已经存储在记录中的文档正文之后。

当 EDD 接收到具有“文件完成”指示符的包后，就知道发送方已经完

成了文档的发送。接着 EDD 通过国际互联网电子邮件将一个到达通知发送给文件的所有接收方，通知他们来了一个文件等待。

到达通知如下:

电子文件到达通知（国际互联网电子邮件消息）

发送方名称，公司，职别，及电子邮件地址

跟踪号码

关于如何接收电子文件的指令。

EDD 还将 EDD 接收方记录的状态更新为“已通知”。当所有的接收方都检索或拒绝电子文件后，DPC 通过互联网电子邮件将一个状态通知发送给文件生成源。

状态通知如下:

电子文件状态通知（互联网电子邮件消息）

发送方名称，公司，职别，及电子邮件地址

跟踪号码

接收方列表，对于每个名称，公司，职别，电子邮件地址

发送日期和状态。

DPC 找到 EDD 机构表中每个个人的公司和职别信息。

1.5.7.17.电子文件检索

电子文件检索请求

BIA 部分:

4 字节 BIA 标识符

4 字节序列码

加密的（DUKPT 密钥）生物特征 - PIC 块:

300 字节授权生物特征

4 - 12 位数字 PIC

56 位响应密钥

跟踪号码

MAC

终端部分:（未使用）

电子文件检索响应

加密的（响应密钥）：

个人代码

56 位消息密钥

状态（未完成，正常，无效接收方）；

MAC

加密的（消息密钥）：

文件正文

DPC 通过执行个人识别过程使用生物特征－ PIC 来识别提出电子文件检索请求的个人。

接着 DPC 找到以跟踪号码和个人生物特征标识为关键字的 EDD 接收方记录。

若不能找到记录，则请求以“无效接收方”状态宣告失败。否则， DPC 将文件的消息密钥及文件（仍由消息密钥加密）发送给请求方。

接着 EDD 将 EDD 接收方记录的状态更新为“已检索”。当所有接收方已经检索或拒绝文件之后， DPC 通过互联网电子邮件将一个状态通知发送给文件生成源（见上面的电子文件数据），并且然后进行调度，删除文件和接收方记录（见安全传真检索）。

1.5.7.18.电子文件拒绝

电子文件拒绝请求

BIA 部分:

4 字节 BIA 标识符

4 字节序列码

加密的（ DUKPT 密钥）生物特征－ PIC 块:

300 字节授权生物特征

4 － 12 位数字 PIC

56 位响应密钥

消息跟踪号码

MAC

终端: （未使用）

电子文件拒绝响应

加密的（响应密钥）:

个人代码

状态代码（正常，无效接收方）

MAC

DPC 使用生物特征－ PIC 来识别提出电子文件拒绝请求的个人。接着 DPC 找到以跟踪号码和个人生物特征标识为关键字的 EDD 接收方记录。若不能找到记录，则请求以“无效接收方”状态宣告失败。

EDD 将 EDD 接收方记录的状态改写为“已拒绝”。接着， DPE 执行如在上面在电子文件检索中所描述相同的通知和删除过程。

1.5.7.19.电子文件存档

电子文件存档请求

BIA 部分:

4 字节 BIA 标识符

4 字节序列码

加密的（ DUKPT 密钥）生物特征－ PIC 块:

300 字节授权生物特征

4 － 12 位数字 PIC

56 位响应密钥

跟踪号码

MAC

终端部分: （未使用）

电子文件存档响应

加密的（响应密钥）:

个人代码

状态代码（正常，无效个人）

MAC

DPC 使用生物特征－ PIC 来识别提出电子文件存档请求的个人。 DPC

找到以请求的传真跟踪号码和个人的生物特征标识为关键字的 EDD 接收方记录。若不能找到记录并且该个人不是发送方或不是接收方之一，则请求以“无效个人”状态而宣告失败。否则， DPC 将文件和接收方记录复制进 EDD 档案数据库。其后对这些记录的任何改变也将被复制进存档版本。

1.5.7.20.电子文件档案检索

电子文件档案检索请求

BIA 部分:

4 字节 BIA 标识

4 字节序列号

加密（ DUKPT 密钥）的生物特征 - PIC 块:

300 字节的授权生物特征

4 - 12 位数字的 PIC

56 位的响应密钥

可选的职别索引代码，发送传真号和扩展跟踪号

MAC

终端部分: （未用）

电子文件档案检索响应

加密（响应密钥）的:

个人代码

状态代码（正常，无效个人）

MAC

该 PPC 能接收来自一个安全传真终端或一个合格的电子邮件终端的电子文件档案检索请求。 DPC 使用个人标识过程来确定发送该档案检索请求的个人。该个人必须是发送方或是接收方中的一个，否则 DPC 拒绝该请求并设置状态代码为“无效个人”。然而，如果该归档的文件是一份用一个公司职别发送的传真， DPC 允许在该公司级别中职别较高的其他个人检索该归档的文件。

EDD 维护一个档案数据库，该数据库的索引是文件的初始跟踪号，存储在如 CD - ROM 和磁带等需要花相当的时间去检索该归档文件的脱机媒介

上。从而， DPC 并不马上返回该归档文件，而是通知请求个人 DPC 已开始搜索。在之后的某一天，等 DPC 完成搜索后，依据原始文件的不同格式，它将通过标准的文件到达通知机制－如传真或电子邮件通知请求方归档文件已检索出来。

DPC 建立一个 EDD 档案请求纪录来存储关于请求方的信息，从而在搜索完成后， DPC 能记得给谁发送检索出来的文件。

1.5.7.21.电子签字

电子签字请求

BIA 部分:

4 字节的 BIA 标识

4 字节的序列号

加密（ DUKPT 密钥）的生物特征－ PIC 块:

300 字节的授权生物特征

4 － 12 位数字的 PIC

56 位的响应密钥

文件名称

文件 MDS 计算

MAC

终端部分: （未用）

电子签字响应

加密（响应密钥）的:

个人代码文本

签字串

MAC

为了处理电子签字请求， DPC 首先用该生物特征－ PIC 完成一个生物特征识别。然后 DPC 建立一个 ESD 记录，给它分配一个唯一的签字标识代码，并在请求中将记录的签字字段设为该电子签字。 DPC 接着返回一个可在以后验证中用的签字串:

“<Dr. Bunsen Honeydew><Explosions in the Laboratory>5/17/95

13 PST 950517000102”

1.5.7.22. 电子签字验证

电子签字验证请求

BIA 部分:

4 字节 BIA 标识

4 字节序列号

加密（ DUKPT 密钥）的生物特征 - PIC 块:

300 字节的授权生物特征

4 - 12 位数字的 PIC

56 位的响应密钥

签字串

MAC

终端部分: （未用）

电子签字验证响应

加密（响应密钥）的:

个人代码文本

签字串

状态（验证通过，失败）

MAC

DPC 完成生物特征识别，从签字串中提取出签字跟踪代码，检索所指明的 ESD 记录并验证其与签字串匹配。 DPC 返回个人代码及签字比较的结果。

1.5.7.23. 网络凭证

网络凭证请求

BIA 部分:

4 字节 BIA 标识

4 字节序列号

加密的（ DUKPT 密钥）生物特征 - PIC 块:

300 字节的授权生物特征

4 - 12 位数字的 PIC

56 位的响应密钥

帐户索引

银行代码

银行主机名称（ hostname ）

终端端口及银行端口（ TCP/IP 地址）

MAC

网络凭证响应

加密的（响应密钥）：

个人代码

签字的（ DPC 的专用密钥）：

凭证（时间，帐户，终端端口，银行端口）

银行的公共密钥

状态代码（正常，失败）

MAC

DPC 对使用请求中的生物特征 - PIC 的个人进行识别并检索存在指定的索引中的个人资产帐户。如果该帐户索引是紧急帐户，则网络凭证响应状态代码被设为“失败”，不产生凭证。

DPC 用当前时间，检索到的资产帐户及终端和银行的 TCP/IP 地址创建凭证。 DPC 然后用公共密钥加密来用它的专用密钥对凭证签字。

响应还包括银行的公共密钥，该公共密钥是 DPC 从远程商户数据库检索出来的。

1.5.8. 客户支持及系统管理消息

DPC 还处理归类为内部消息的辅助消息类型。 DPC 一般不从非 DPC 系统接受这类消息。这类消息随数据库供应商的不同而不同。然而，内部网络使用 DES 加密包来提供附加安全度。

客户服务及系统管理任务是用数据库供应商的查询语言及应用开发工具来实现的。

1.5.8.1.客户服务任务:

- IBD: 查找，激活，去激活，删除，更新记录
- AID: 增加或删除授权个人
- AOD: 查找，增加，删除，更新记录
- VAD: 查找，激活，去激活，删除，更新记录
- RMD: 查找，增加，删除，更新记录
- PFD: 增加，删除，更新记录

1.5.8.2.系统管理任务:

- 欺诈预检查
- 修改有效站点列表
- 总结日志信息（警告，错误，等）
- 修改 PIC 组列表
- 性能监控
- 进行备份
- 事故恢复过程
- DPC 站点的时间同步
- 改变主登记站点
- 改变秘密 DES 加密密钥
- 清除旧文件跟踪号
- 产生一个 BIA 硬件标识代码、MAC 加密密钥和 DUKPT 基密钥三者的列表。存储在密钥加载设备的加密软盘上。

1.5.9.防火墙机

1.5.9.1.目的

防火墙（ FW ）机提供对付网络病毒和计算机黑客的防护第一线。所有进出 DPC 站点的通信链路首先通过一个安全 FW 机。

1.5.9.2.用法

FW 机是一个互联网－局域网路由器，只处理到达 GM 机的消息。

配备 BIA 的终端通过调制解调器，X.25 或另外的通信介质给单个 DPC 站点发送包。DPC 依靠第三方来提供所需的调制解调器库以处理大量的呼叫并把数据送到 DPC 主干。

对于主要用于分布式事务和序列号更新的 DPC 到 DPC 通信，FW 机发送长度加倍的 DES 加密包。DPC LAN 部件处理加密和解密：FW 没有对包进行解密的能力。

1.5.9.3. 安全性

一个适当构造的网络嗅探器（sniffer）作为 FW 的后备保险装置，用来检测入侵者。若检测到匿名消息，该入侵消息整体地都被记录下来，并提醒操作者，而且嗅探器会从物理上关掉 FW 机。

FW 不允许任何从内部网到互联网其余部分的传输。

1.5.9.4. 消息带宽

交易授权请求需要大约 400 字节，登记包大约需要 2KB。为了能每秒处理 1000 个交易授权及每秒一个登记包，FW 机能每秒处理大约 400KB（在该领域熟知）。

每个 DPC 站点需要将近 3 个到第三方调制解调器库和其他 DPC 站点的 T1 连接的集中带宽。

1.5.10. 网关机

1.5.10.1. 目的

GM 机（GM）通过 FM 机把外部世界（配备 BIA 的终端和另外 DPC）链接到 DPC 的内部组成部分。DPC 有多个 GM，通常为两个。

1.5.10.2. 用法

GM 负责每个 BIA 请求的处理，与各 DPC 组成部分进行必要的通信，并把加密的请求结果送回请求发送方。完成这一任务的软件称作消息处理模块。

GM 记录下所有它所接收到的请求及从它所通信的组成部分收到的任何警告。例如， GM 记录下任何紧急帐户访问，序列号断缺及无效包。

该 GM 在处理一个请求时可能需要通知在所有另外 DPC 中的 GM，该 DPC 数据库发生了变化。当发生这种情况时，该 GM 运行一个分布式事务以更新那些远程数据库。

分布式事务分为两类：同步的和异步的。同步分布式事务需要该 GM 在继续处理包以前等待该分布式事务的提交。异步分布式事务不需要 GM 等待提交，而允许 GM 完成请求的处理而不管分布式事务是否已提交。异步分布式事务只用于更新那些对于数据库一致性并不是绝对需要的数据：对序列号和生物特征检查和的记录可以异步进行，而创建如个人生物特征记录等的数据库记录则需要同步进行。

在执行一个同步分布式事务时，发请求的 GM 只在所有站点都能在本地成功地提交事务时才认为整个事务成功。否则，这些 GM 都恢复本地数据的改变并由于事务错误而拒绝请求。

有效 DPC 站点列表通常包括所有的站点。然而在站点严重故障的情况下，系统管理员可以从该有效站点列表中手工删去该站点。然而分布式事务失败最常见的原因是与任何 DPC 设备都无关的临时网络故障。在网络连接恢复前或该站点从有效站点列表中删除前，不能执行需要同步分布式事务的请求。系统管理员在把一个站点加回到有效站点到表中以前，将把该站点数据库更新到与当前活动站点的数据库一致。

1.5.10.3. 软件组成部分

为了提高性能，每个 GM 都本地运行下列软件组成部分：

消息处理模块

消息鉴别代码模块

消息解密模块

个人生物特征数据库机列表

1.5.10.4. 消息带宽

GM 所需的消息带宽与 FW 机所需的带宽类似。一个 FDDI 网络接口可提

供每秒100Mb的带宽，能很容易满足任何带宽需求。

1.5.11.DPC LAN

1.5.11.1.目的

DPC局域网（LAN）用光纤令牌环把DPC站点的机器连起来。光纤令牌环能提供很高的带宽和很好的物理安全性。

1.5.11.2.安全性

DPC LAN上的机器所用的网络接口包括解密硬件以使侦听或监听包因没有加密密钥而无用。加密密钥存在加密硬件中，并对LAN上的所有机器都一样。

一个适当构造的网络嗅探器作为FW的后备保险装置，用来探测入侵者。若检测到一匿名消息，该入侵消息整个都会被记录下来，并提醒操作员，而且该嗅探器还将物理关闭该FW机。

j1.5.12.消息处理模块

1.5.12.1.目的

消息处理模块（MPM）负责处理请求。在必要时它与DPC的其他组成部分通信以完成其任务。MPM在机器上被标为GM。

1.5.12.2.用法

MPM对每一个当前正在处理的请求维护一个请求上下文。该请求上下文包括为维护到发出请求的终端的网络联接的必要信息，BIA设备信息，响应密钥和响应包。

1.5.13.消息鉴别代码模块

1.5.13.1.目的

消息鉴别代码模块（MACM）的任务是验证在入站包上的消息鉴别代码以及将一个消息鉴别代码加到出站包。

1.5.13.2.用法

MACM 维持一个由 BIA 硬件标识码作为关键字的 112 位 MAC 加密密钥的位于内存的散列表。

当 MACM 从 GM 接收一个请求以确认一个包的 MAC 时，它首先在散列表中查找该包的硬件标识码。如果没有表项，则 MACM 以“无效硬件标识码”错误回答 GM。

否则，MACM 使用 112 位 MAC 加密密钥对包的 BIA 消息息部分进行 MAC 检查。如果 MAC 检查失败，则 MACM 以“无效 MAC”错误回答 GM。否则，MACM 以“有效 MAC”消息回答。

如果包中含有商户代码，MACM 也对照散列表中的拥有者标识码检查商户代码。如果码不匹配，则 MACM 以“无效拥有者”错误回答。

当 MACM 从 GM 接收一个请求，为一个包产生 MAC 时，它用包的硬件标识码查找 MAC 加密密钥。用 MAC 加密密钥，MACM 产生一个 MAC 并将之加到该包。如果 MACM 不能在它的散列表中发现该硬件标识码，它就以无效硬件标识码错误回答。

1.5.13.3. 数据库模式

MACM 散列表表项包含:

MACM 表项:

硬件 Id=int4

拥有者 Id=int4

mac 加密密钥=int16

该表由硬件标识码散列而成。

1.5.13.4. 数据库大小

假设使用了 5 百万个配备有 BIA 的设备，散列表需要有大约 120MB 的存储量。考虑到性能因素，这个散列表完全设在存储器中的高速缓存区。

1.5.13.5. 依赖性

MACM 只含有涉及有效 BIA 硬件标识码和有效设备拥有者的记录。当一个设备或设备拥有者已挂起或从系统中消除时，MACM 就将任何涉及该标识

码的表项移去。当一个设备被启动时，MACM 则为它加入表项。

MACM 还从有效设备数据库中对 MAC 加密密钥进行高速缓存。由于系统不允许修改 BIA 的密钥，所以无须担忧 MACM 接收到密钥更新。

1.5.14. 消息解密组件

1.5.14.1. 目的

消息解密组件（MDM）任务是重建 DUKPT 交易密钥并用它对包中的生物特征－ PIC 块进行解密。它维持一个 DUKPT 基本密钥列表，这是产生交易密钥所需的。

1.5.14.2. 用法

MDM 使用包的序列号作为 DJKPT 交易计数、用 BIA 硬件标识码的高 22 位作为 DUKPT 抗窜改安全模块（或“TRSM”）标识、并用 BIA 硬件标识码的低 10 位作为 DUKPT 密钥设定标识来组建 DUKPT 交易密钥。

DUKPT 标准规范了如何产生交易密钥。密钥设定标识用于从基本密钥列表中查找出一个基本密钥。基本密钥用于将 TRSM 标识通过加密/解密/加密循环变换成初始密钥。然后，交易计数器按 DES 加密/解密/加密循环系列施加给初始密钥，以产生交易密钥。

为了增加安全性，维持二个基本密钥表，一个用于低安全性 BIA 设备，一个用于高安全性设备。MDM 根据设备的安全级别选择使用哪一个基本密钥表。

1.5.14.3. 数据库模式

MDM 基本密钥表表项包含:

MDM 表项:

基本密钥=int16

基本密钥表由密钥设定标识加索引。

1.5.14.4. 数据库大小

MDM 维持 DUKPT 基本密钥的位于内存中的列表。每一密钥需要 112 位。

MDM 维持二套 1024 密钥，总共需要 32KB。

1.5.14.5.依赖性

MDM 不直接依赖其他任何 DPC 部件。

1.5.15.PIC 组列表

1.5.15.1.目的

PIC 组列表（ PGL ）与个人生物特征数据库机列表一起定义 IBD 机器结构。 PGL 在系统中存储 PIC 组列表用于简化 PIC 管理。 PIC 组是一套连续的 PIC 码。 PGL 存在于每一个 GM 机（ GM ）中。

1.5.15.2.用法

当给定一个 PIC 码时， PGL 就通过其 PIC 组列表查找含有该 PIC 码的组。 PGL 按顺序维持组的列表，并使用二进制检索快速发现正确的组。

PGL 的初始结构是一个包含所有可能的 PIC 的巨 PIC 组。在分配了临界量的 PIC 之后，巨 PIC 组分裂成二个。其后这一过程施加给后续所有 PIC 组。

在 PIC 组分裂时， PGL 根据先来优先原则基于可用存储器指定新的主机和备用 IBD 机。 PCL 协同 IBD 机首先从旧的主及备用机中复制涉及的记录到新机中，更新 IML 记录，最后去除旧主机及备用机中的拷贝。分裂 PIC 组是一个自行任务。当 DPC 有轻负荷时，如在夜里， PGL 批量处理待进行的分裂请求。

对于给定的 PIC 组，如果机器的自由存储区低于预期处理新登记所需水平时，系统管理员也可改变主机及备用 IBD 机。

1.5.15.3.数据库模式

PIC 组记录的模式是

PICGroup:

低 Pin=int8

高 Pin=int8

used=int4

每一个 PIC 组由唯一的标识确定。为了方便起见， PIC 组标识码是该组的低 Pin 码，然而系统不必基于此。

PCL 以低 Pin 字段为关键字。

1.5.15.4. 数据库大小

期望 PGL 包含约 3000 个组（每一 PIC 组包含约 1000 个有效 PIC，但可跨越几百万个实际 PIC）。整个 PGL 需要约 72KB 的存储量并完全高速缓存于存储器中。

1.5.15.5. 依赖性

当增加，合并、或分裂 PIC 列表时， PGL 负责通知 IBD 列表变化并指引 IBD 记录从一个 IBD 机移向另一个。

1.5.16. 个人生物特征数据库机器列表

1.5.16.1. 目的

IBD 机器列表（ IML ），与 PIC 组列表一起编码 IBD 机器结构。 IML 将 PIC 码映射到存有 PIC 的 IBD 记录的主和备用 IBD 机中。 IML 实际以 PIC 组（一套连续的 PIC 码）而不是以个人的 PIC 为关键字，因为这可大大节省存储列表所需的存储空间。 IMC 存在于每一个 GM 机器（ GM ）上。

1.5.16.2. 用法

当 GM 处理到一个要求生物特征识别的请求时， GM 找到以生物特征的 PIC 组为关键字的 IML 记录。然后 GM 知道了用于生物特征识别的主机与备用 IBD 机器。

1.5.16.3. 数据库模式

IML 表表项的模式是:

机器对:

pin 组=int8

主=int2

备用=int2

IML 以 pin 组为关键字。

1.5.16.4.数据库大小

希望 IML 包括约 3000 个表项（ PIC 组的数目）。每一机器对记录是 12 字节，需要约 36KB 的存储量，并完全高速缓存于存储器中。

1.5.16.5.依赖性

IBD 机器结构中任何变化都反映到 IML 中。此外， IML 使用 PIC 组为关键字，当 PIC 组列表有变化时， IML 也被更新。

1.5.17.序列号模块

1.5.17.1.目的

序列号模块（ SNM ）的主要功能是判断包序列号的有效以防止重复的攻击。其第二个任务是通知远程 DPC 站点中的其他 SNM 序列号更新，将再次提交攻击的影响降至最小，并周期地更新有效设备数据库中的序列号。

SNM 维持序列号的位于内存的散列表，以 BIA 硬件标识码为关键字，以便快速确认包序列号。

1.5.17.2.用法

当 SNM 从 GM 接收到一个就给定硬件标识码和序列号确认有效的请求时，它在散列表中查找该硬件标识码。如果没有 SNM 就回答 GM “无效硬件标识码”错误。

否则， SNM 对照散列表表项中存储的序列号检查这个给定序列号。如果序列号小于或等于存储的序列号，则 SNM 回答“无效序列号”错误。否则， SNM 将散列表表项中的序列号设置为给定序列号，并以“有效序列号”消息回答。

有时 SNM 可观察到序列号空缺。当 SNM 收到一个序列号，比散列表表项中的序列号大于一以上时，就有序列号空缺发生。换言之，有序列号被

略过。SNM 发现序列号空缺时，它回答“序列号空缺”消息给 GM，而不是“有效序列号”消息。GM 将包作为有效处理但标以“序列号空缺”警告。

序列号空缺通常发生在，网络连接状态的丢失时；即在网络恢复到工作秩序之前掉包或不能发出。然而，序列号空缺也可因欺诈而发生：恶意方可截获包，使它们不能到达 DPC 或者他们企图伪造包（用大序列号使它不会被立即拒绝）。

SNM 的第二功能是通知其他 DPC 更新后的序列号。当只有第一站点应接收包时，在所有 DPC 站点快速更新序列号可抵抗再提交攻击，这种攻击中恶意者监视以一个 DPC 站点为目的地的包，并立即向一个不同的 DPC 站点发送一个复制包，以期利用从一个 DPC 站点向另一个站点传送序列号的延迟，达到两个站点都接受该包为有效。

无论何时收到有效序列号时，SNM 相互发送更新消息。如果一个 SNM 收到一个序列号的更新消息，该序列号小于或等于散列表中当前存储的序列号，该 SNM 记录序列号再次提交警告。所有再次提交攻击都是这样得以检测的。

完全抵抗再次提交攻击更简单的方法是只让一个 SNM 确定包的有效。在这种方案中，没有更新传输延迟窗口可被利用来进行再次提交攻击。或者，许多 SNM 同时工作，只是它们不能为同一装备 BIA 的设备确认序列号。

1.5.17.3.序列号维护

当 SNM 启动时，它从 VAD 中存储的有效 BIA 的序列号中装入序列号散列表。

每日一次，SNM 将当前序列号下载到本地有效设备数据库（VAD）中。

VAD 负责为任何工作或停止的备有 BIA 的设备的 SNM 发送增加表项和去除表项消息，以保持 SNM 散列表最新。

1.5.17.4.数据库模式

SNM 散列表表项包含：

SNM 表项：

硬件 Id=int4

序列号=int4

散列表以硬件 Id 为关键字。

1.5.17.5.数据库大小

若有约 5 百万个备有 BIA 的设备投入使用，则需散列表约 40MB 。

1.5.17.6.依赖性

SNM 依靠有效设备数据库。当一个设备挂起或从数据库移走， SNM 去除对应的表项。当激活一个设备， SNM 为其建立一个表项。

1.5.17.7.消息带宽

SNM 需要每秒约 8KB 的传输带宽来处理每秒 1000 个更新序列号消息。更新序列号消息被缓存并每秒发送一次以便将实发消息数目降至最少。

1.5.18.设备拥有者数据库

1.5.18.1.目的

设备拥有者数据库（ ADD ）存储关于拥有 1 个或多个备有 BIA 的设备的个人或机构的信息。这些信息用于双重检验 BIA 设备只由正当拥有者所用、为金融借贷交易提供资产帐户信息，并对特定个人或机构所拥有的所有 BIA 设备可进行识别。

1.5.18.2.用法

每个 ADD 记录包括当 DPC 处理拥有者的备有 BIA 的设备之一提交的金融交易时向拥有者贷或借的资产帐户。例如，从零售点终端的 BIA 提出交易涉及贷给资产帐户，而验证的电子邮件传输导致将帐记入资产帐户。

1.5.18.3.数据库模式

设备拥有者记录模式是:

设备拥有者:

拥有者 Id=int4

名称=char50

地址=char50

邮政编码=char9

资产帐户=char16

状态=int1

状态字段是如下之一:

0: 挂起

1: 活动

设备拥有者数据库是以拥有者 Id 为关键字.

1.5.18.4.数据库大小

希望 AOD 存储约 2 百万个设备拥有者记录。每个表项 130 字节，需要约 260MB 存储量。 AOD 以拥有者标识码为关键字的散列文件被存储。 AOD 的副本存在每个 GM 上。

1.5.18.5.依赖性

当表项从 AOD 去除或挂起，任何涉及这些设备拥有者的有效设备数据库记录都标以挂起。此外， MAC 模块和序列号模块都去除挂起设备的表项。

1.5.19.有效设备数据库

1.5.19.1.目的

有效设备数据库（ VAD ）是表示所有至今制造出的 BIA 的记录集合。VAD 对每一个 BIA 记录包含消息鉴定码加密密钥，以及一个指示 BIA 是否激活、等待运输或被破坏的指示。为了把来自 BIA 的消息解密， BIA 必须存在并且在 VAD 中有一个激活的记录

1.5.19.2.用法

制造时，每个 BIA 有唯一的公共识别码和唯一的 MAC 加密密钥。两者都先于 BIA 使用被输入 VAD 记录中。

当一个BIA首先构成时，它被给与一个唯一的硬件标识码。当BIA投入使用时，其硬件标识码由系统登记。首先，将BIA的所有者或负责方输入设备所有者数据库（AOD）。然后，VAD记录指向AOD记录，并且BIA设置为激活。来自那个BIA的请求被DPC接受。

当BIA离开服务时，它被标记为未激活，并且至AOD记录的链接断开。没有从BIA接受通信、

每个BIA类型和模型都有赋予它的安全级，指示其物理安全级。当DPC处理来自那个BIA的请求时，它使用BIA的安全级测量何种行为是允许的。DPC也对外部金融交易授权服务机构提供安全级。

例如，金融交易授权服务机构能够拒绝来自低安全级BIA的任何超过$ 300的请求，要求个人使用更高安全级的BIA以授权这样的额度。授权服务机构也能够使用安全级作为基于风险的交易支付量的指导。

他们允许的安全级和行为是实际确定的。实际上，欺诈系统的成本必须高于潜在收益，所以安全级与成本相联以与设备折衷。

1.5.19.3.数据库模式

有效设备记录的模式是:

有效设备:

硬件Id=int4

mac加密密钥=int16

拥有者Id=int8

制造日期=int8

服役日期=time

安全级别=int2

状态=int1

类型=int1

使用=int1

状态字段可能值是:

0：挂起

1：激活

2：破坏

类型字段可能值是（每个类型的终端一个）

0： ATM

1： BRT

2： CET

3： CPT

4： CST

5： EST

6： IPT

7： IT

8： ITT

9： PPT

10： RPT

11： SFT

使用字段可能值是：

0：零售

1：个人

2：发行人

3：远程

有效设备数据库由硬件识别码作为关键字。

1.5.19.4.数据库大小

VAD 大约处理 500 万零售、发行人及远程有效设备条目，每个条目是 51 字节，共需 255MB。VAD 作为由硬件识别码为关键字的散列文件而被存储。VAD 的一个拷贝被存在每一个 GM 上。

在 3 千万范围内的个人有效设备条目数的数量，需要另一个 1.5GB 的存储量。

1.5.19.5.依赖性

当 VAD 记录改变状态时，MAC 模块和序列号模块被通知其状态的改

变。例如，当设备变为激活时， MACP 和 SNM 为新激活的设备加入一个条目。当设备变为未激活时， MACP 和 SNM 为该备除掉其条目。

1.5.20. 个人生物特征数据库

1.5.20.1. 目的

个人生物特征数据库（ IBD ）记录存储个人信息，包括它们的主和辅生物特征数据、 PIC 码、金融资产帐户列表、专用代码、紧急帐户、地址及电话号码。个人也以有选择地包含它们的 SSN 和电子邮件地址。这一信息对于通过或者生物特征或者个人信息识别一个个人、访问帐户信息、或为远程商户提供一个地址或电话号码用于附加验证是必要的。

1.5.20.2. 用法

在个人登记过程中，个人在世界范围内的零售银行机构或本地系统机关已登记的生物特征登记终端处被加到系统中。在注册期间，个人选择其个人识别号，并且把金融资产帐户加到其生物特征和 PIC 组合数据中。

个人信息在由任何发行成员报告有欺诈行为时均可以从数据库中除掉。如果这种情况出现，该个人的帐户信息被授权的内部系统代表从 IBD 中移到先前欺诈数据库（ PFD ）中。在 PFD 中记录的生物特征标识不能用于 IBD 中的记录。

IBD 存在于多个机器上，每一个机器负责 IBD 记录的一个子集，每个记录的拷贝存储在两个不同的机器上，两者用于冗余和负载共享。存储在 GM 上的 IBD 机器列表，维持哪一个机器保持哪一个 PIC 。

1.5.20.3. 数据库模式

用于个人生物特征记录的模式是:

个人生物特征:

主生物特征=biometric

辅生物特征=biometric

生物特征 Id=int4

PIC=char10

电话号码=char12

姓=char24

名=char24

中间名=char2

SSN=char9

专用代码=char40

地址=char50

邮政编码=char9

公共密钥=char64

检查和=int4[10]

帐户链接=char30[10]

紧急索引=char1

紧急链接=char1

特权=char10

注册者=int8

紧急使用计数=int4

状态=int1

状态字段之一是:

0: 挂起

1: 活动

2: 先前欺诈

IBD 由 PIC 作为关键字。

1.5.20.4. 数据库索引

每个 IBD 机器有另外的关于个人社会安全号、生物特征识别码、姓、名及电话号码的索引以便于对 IBD 数据库的访问。

1.5.20.5. 数据库大小

每个 IBD 机器有由一个或多个 RAID 设备提供的 40GB 的二级存储器。每个 IBD 记录 2658 字节（假设生物特征数据每条是 1K），允许每个机器

有高达1500万个记录。IBD记录使用(也许是成簇的)二级索引存储在PIC上，该索引存在存储器中并且需要不大于64MB的存储量（64MB索引管理大约1600万的项）。为了对3亿个人存储记录，DPC至少需要40个IBD机器：20个IBD机器用于主存储器，另外20个用于备份。IBD机器的数量很容易根据登记的个人的数量进行增减。

1.5.20.6.依赖性

IBD机器、PIC组列表及IBD机器列表利用哪一个PIC是在哪一个机器上保持最新。当PIC组重新配置或用于PIC组的主和备份机器变化时，IBD机适当更新其数据库和索引。

1.5.21.授权个人数据库

1.5.21.1.目的

对每个发行人或个人备有BIA的设备，授权个人数据库（AID）保存了由设备拥有者授权使用它的个人的列表。

AID存在的原因有两个。第一个是它提供了限制访问终端。例如，发行人终端只能由授权的银行代表使用。关于AID的第二个原因是，防止罪犯用电话终端的个人BIA秘密替换零售点销售终端中的BIA，然后把所有的款项转移到由罪犯建立的远程商户帐户上。

1.5.21.2.数据库模式

授权个人数据模式是:

授权个人:

硬件 Id=int4

生物特征 Id=int4

硬件Id是指在有效设备数据库中的一个记录，以及生物特征Id是指在个人数据统计数据库中的一个记录。任何时候DPC都需要检验一个个人是否被授权使用一个个人或发行人设备，DPC用正确的硬件Id和生物特征Id检验授权个人记录的存在。

个人BIA设备由在有效设备数据库中设有1（个人）的使用字段识别。发行人BIA设备由在有效设备数据库中设为2（发行人）的使用字段识别。

1.5.21.3.数据库大小

假设每个发行人终端有 10 个授权使用它的个人，并且每个人设备有两个另外的授权个人，服务器中有 1,000,000 个个人设备，则 AID 存储了大约:

$10 \times 100,000 + 2 \times 1,000,000 = 3,000,000$ 项

整个数据库需要大约 24MB 的存储量。

1.5.21.4.依赖性

当授权拥有者数据库记录或有效设备数据库记录被去除时，所有参考它们的授权个人记录被去除。

1.5.22.先前欺诈数据库

1.5.22.1.目的

先前欺诈数据库（ PFD ）是一个表示过去在某个点欺诈发行人成员的个人的记录的集合。 PFD 也在系统的低激活期间运行后台交易以在 IBD 中清除那些在 PFD 中有匹配记录的个人。

系统不会把个人自动放入 PFD 中，除非它检测到他们试图重新登记，把个人放入 PFD 中是一个敏感的政策问题，超出了本文的范围。

1.5.22.2.用法

在一个新的 IBD 记录被为激活之前，使用如在个人识别过程中用过的相同生物特征比较技术把个人的初级和二级生物特征数据对每一在 PFD 中的生物特征数据作检验。如果发现了新 IBD 记录的一个匹配， IBD 记录的状态被设为“先前欺诈”。如果先前欺诈检验被作为登记请求的一部分进行， GM 记录一个“登记一个有先前欺诈的个人”的警告。

假设 PFD 将保持相对小。运行 PFD 的成本是昂贵的，因为它是一个偶然生物特征检索，所以只把那些对系统增加了明显的耗费的个人加入 PFD 中。

1.5.22.3.数据库模式

先前欺诈记录模式是:

先前欺诈:

主生物特征=biometric

辅生物特征=biometric

生物特征 Id=int4

PIC=char10

电话号码=char12

姓=char24

名=char24

中间名=char2

SSN=char9

专用信号=char40

地址=char50

邮政编码=char9

公共密钥=char64

检查和=int4[10]

帐户链接=char30[10]

紧急索引=char1

紧急链接=char1

特权=char10

注册者=int8

紧急使用计数=int4

状态=int1

状态字段之一是:

0: 挂起

1: 活动

2: 先前欺诈

PFD 由生物识别码作为关键字.

1.5.22.4.数据库大小

PFD 记录与 IBD 记录相同。有幸的是， DPC 只需存储其一小部分，所以只需两台数据库机器存储整个数据库，其中一个是备份。

1.5.22.5.依赖性

PFD 对任何其他的 DPC 成分没有任何直接的相关性。

1.5.23.发行人数据库

1.5.23.1.目的

发行人数据库（ ID ）存储关于其资产帐户允许通过系统访问的银行和其他金融机构的信息。发布机构是唯一能够把其资产帐户数加入或移出给定个人的 IBD 记录的机构。

1.5.23.2.用法

DPC 使用 ID 通过在 ID 中搜索一个含有发行人终端的发行人码的一个记录来确认来自发行人终端的请求。存储在记录中的拥有者标识必须与存储在发行人终端中的 BIA 有效设备数据库中所存的拥有者相匹配。

发行人记录是:

发行人记录:

发行人代码=int6

拥有者 Id=int4

姓名=char50

电话号码=char12

地址=char50

邮政编码=char9

发行人数据库由发行人代码作为关键字。

1.5.23.3.数据库大小

发行人数据库处理大约 100,000 个表项。每个表项是 127 字节，需要小于 2MB 。 ID 的拷贝存在每个 CM 上。

1.5.23.4.依赖性

发行人数据库对任何其他DPC成分没有任何直接依赖性。

1.5.24.电子文件数据库

1.5.24.1.目的

电子文件数据库（EDD）存储和跟踪电子文件，如给特定个人的传真图象和电子邮件消息。它也保持企业机构图以提供发送方和接收方两者的官方职别。EDD也以发送方或接收方的请求存档文件并且提供通过系统提交的合同协议的中立的第三方验证。

1.5.24.2.用法

当DPC从某人接收一个传真或者其它电子文件时，它产生一个EDD文件记录来存储该文件，直到该文件被一个授权的接收方获取。

对于传真文件，接收方是由传真号和扩展名规定的。对于其它电子文件，接收方是由电子邮件地址规定的。DPC利用传真号和扩展名或者电子邮件地址查找每个接收方的机构记录。如果找不到记录，则仅当接收方是由电子邮件地址规定的时，则DPC从个人生物特征数据库中查找。如果找到的话，对于每个接收方，DPC生成一个涉及该文件和由机构或者IBD记录规定的接收方生物特征数据标识的接收方记录。PC允许未在系统中登记的接收方，但是，不能保证传送或者对接收方的保密性。

EDD是足够灵活的，可以保证传真文件被发送到某人的电子邮件地址，以及将电子邮件消息发送到传真机。

当系统没有在文件上设置电子签字时，系统通过加密毫无疑问地可以保证由验证电子邮件或者安全传真终端接收（并解密的）的消息是由所述的个人发送的。

所述机构的经过授权的官员可以向DPC提交安全传真或者电子消息，向新的成员指派职别和传真扩展名，更新成员的职别或者传真扩展名，或者去除终止的成员。

当某人被从机构树去除时，DPC在一年的周期内放弃扩展号。该退休周期允许个人有足够的时间通知其朋友其将不能在该扩展名接收保密的传

真，使得所述机构不至于错误地将传真发送到该扩展名上的其他人，而使其他人收到不是给他或她的传真.

EDD 在发送方或者文件的接收方之一请求时维护包含文件和接收方记录的副本的归档文件数据库。该归档文件数据库被周期地移送到 CD - ROM 上。

1.5.24.3.数据库模式

EDD 具有三种记录类型:

文件记录:

文件号= int8

发送方 Id= int4

文件传真=fax

文件文本= text

消息密钥= int8

状态= int1

接收方记录

文件号= int8

接收方 Id= int4

接收方传真号=char12

接收方传真扩展名=char8

接收方电子邮件地址= text

接到方= int4

最后修改= time

传送状态= int1

合同状态= int1

归档请求记录:

生物特征数据 Id= int4

文件号= int8

请求方传真号=char12

请求方传真扩展名=char8

请求方电子邮件地址=text

机构记录:

生物特征数据 Id=int4

登记人=int4

公司=text

职别=text

传真号=char12

传真扩展名=char8

电子邮件地址=text

有效日期=time

privs=int2

状态=int1

文件记录状态字段为下列之一:

0: 未完成

1: 正常

接收方记录传送状态字段为下列之一:

0: 未完成

1: 通知的

2: 拒绝的

3: 检索的

4: 检索的不安全的

5: 忙的

接收方记录合同状态字段为下列之一:

0: 无

1: 接受

2: 拒绝

机构记录状态字段为下列之一:

0: 有效的

1: 挂起的

机构记录特权字段是用于指示 DPC 允许所述个人那些特权:

0： 登记

文件、接收方和归档检索记录由文件号作为关键字。机构记录由生物特征数据 Id 作为关键字。 EDD 维护发送方 Id 字段、接收方接收方 Id 字段、机构公司名称和职别字段上的二级索引。

1.5.24.4.数据库大小

由于电子邮件消息与传真页相比较相对较小，所以 EDD 存储的需求主要取决于需要存储的传真页的数目。每个传真页需要大于需要 110K B 的存储量。假定每个传真有 4 页，每个人每天两个传真，和 3000 万台传真机，EDD 需要 24G B 的存储量来存放一天的传真。

1.5.24.5.安全性

利用 B IA 加密机制加密，文件被发送到系统以及从系统发出。但是，加密密钥被存放在与文件相同的数据库。文件被保持在加密状态以避免偶然的泄漏，但是关心存放在系统的文件的安全的人们自己应当设置额外的加密。

1.5.24.6.消息带宽

每个传真需要大约 110K B ，意味着为一个 T1 连接，具有 1.54M B/秒的吞吐量，每秒钟可以处理大约 1.75 个传真页。

1.5.25.电子签字数据库

1.5.25.1.目的

电子签字数据库（ ESD ）鉴别并跟踪由系统生成的所有电子签字。

1.5.25.2.用法

作为系统成员的个人，连同生物特征数据 PIC ，为文件提交一个 16 字节的“消息摘要”并获得一个“数字签字”，永久地保持在系统的文件中。该数字签字对个人的姓名、生物特征数据识别代码、授权的签字记录号、文件标题以及对文件签字时的时间标记编码。

为了验证签字，文件的消息摘要首先被计算（例如利用RSA 的MD5），并连同文件的签字标签一起发送。ESD 查找签字标签并根据存储在数据库中的消息摘要验证刚刚计算的消息摘要。

1.5.25.3.数据库模式

用于电子邮件记录的模式是:

电子签字:

签字号=int8

签字人=int4

文件名=text

检查和=int16

日期=time

签字人是给文件签字的个人的生物特征标识代码。电子签字记录由签字号散列的。

1.5.25.4.数据库大小

对于每个1GB 的二级存储器，电子签字数据库存储二百七十万个记录（每个记录大约为32 字节）。

1.5.25.5.依赖性

ESD 依赖于签字人的生物特征标识。由于这些签字永久保持有效，当系统删除签字人的个人生物特征数据库记录时ESD 记录不被去除。注意这需要IBD 永不再用生物特征数据标识。

1.5.26.远程商户数据库

1.5.26.1.目的

远程商户数据库（RMD）存储通过电话，有线电视网络或者国际互联网提供商品和服务的商户的信息。由个人通过适当配备的终端发出的每个定单通过商户定单终端引导至系统。

1.5.26.2.用法

当收到一个个人远程交易授权以及由DPC 验证的MAC 时，商户代码与 RMD 中的商户代码比较。商户代码，可以是电话号码、商户－产品凭证或是国际互联网地址，以正确的商户识别代码的形式存在于 RMD 中，否则DPC 中断请求并向发送BIA 终端设备返回一个无效商户代码错误。

1.5.26.3.数据库模式

用于远程商户记录的模式为:

远程商户:

商户 Id=int4

商户代码=char16

商户类型=int1

公共密钥=int16

远程商户商户类型为下列之一:

0： 电话

1： CATV

2： 国际互联网

商户 Id 和商户代码都为主要密钥。没有具有相同的商户 Id 和商户代码结合的两个RMD 记录。

1.5.26.4.数据库大小

假定有大约100,000 个远程商户， RMD 对于每个记录大约24 字节，总共需要2.4MB 存储量。

1.5.26.5 依赖性

RMD 没有对任何其他DPC 部分的直接依赖性。

1.5.27.系统性能

主要的性能指标是DPC 每秒钟可以处理多少个金融授权交易。

在GM 中:

1.MACM 检验MAC（本地）

2.SNM 检验序列号（网络消息）

3.MDM 对生物特征数据PIC 块解密（本地）

4. 找出 IBD 设备（本地）

5. 向 IBD 设备发送识别请求（网络消息）

在 IBD 设备中:

6. 为 PIC 检索所有的 IBD 记录（x 次寻找以及 x 次读取，其中 x 为存储生物特征数据记录所需的页数）。

7. 对每个记录，比较其主要生物特征数据（y/2m s，其中 y 是检索的记录的数目）。

8. 如果没有合理的匹配，重复步骤 9 但是比较辅生物特征数据（z*y/2m s，其中 y 为检索的记录数目而 z 是未发现匹配的可能性）。

9. 更新最佳匹配 IBD 记录检查和队列并检验可能的重播攻击（1 寻找，1 读取，和 1 写入）。

10. 返回最佳匹配 IBD 记录或者如果匹配不是足够接近反回出错信息（网络消息）。

在GM 中:

11. 利用外部处理器进行授权请求（网络消息）

12.GM 加密以及MAC 响应（本地）。

13. 发送回响应包（网络消息）。

盘总需求

$$x*(s+r)+y/2*(1+z)+s+r+w+5*n$$

$$=(x+1)*(s+r)+y/2*(1+z)+w+5*n$$

[假定 x 为 20, y 为 30, z 为 5 %; s=10m s, r=0m s, w=0m s, n=0m s]

$$=21*10m\ s+15*1.05m\ s$$

$$=226m\ s$$

$$=4.4TPS$$

[假定 x 为 10, y 为 15, z 为 5 %; s=10m s, r=0m s, w=0m s, n=0m s]

$$=11*10m\ s+7.5*1.05m\ s$$

$$=118m\ s$$

=8.4TPS

[假定 x 为 1,y 为 1,z 为 5 %;s=10m s, r=0m s,w =0m s,n=0m s]

=2*10m s+1/1.05m s

=21m s

=47TPS

后备 IBD 设备也处理请求双倍有效TPS。

最坏的情况（两台设备都在使用中）：

每个PIC 的人数	TPS
30	8
15	16
1	94

平均情况（有 20 台机器在使用）：

每个PIC 的人数	TPS
30	88
15	168
1	940

最佳情况（有 40 台机器在使用）：

每个PIC 的人数	TPS
30	176
15	336
1	1880

上述的只是可按有商业前途方式实现的系统的一种配置的例子。但是，可以预计本发明可以以多种方式配置，例如利用更快的计算机、更多的计算机以及其他改变。

1.6.终端协议流程

下面的一组协议流程描述了特定的终端、DPC、附加的BIA 和其他各方例如贷方/借方处理器等等之间的交互作用。

1.6.1 零售销售点终端

在该例中，RPT 与零售BIA 和DPC 通信以授权交易。交易量为452.33，个人帐户为4024-2256-5521-1212,商户代码为123456,个人专用代码为“我已完全被说服”。

RPT → BIA 设置语言<英语>

BIA → RPT 可以

RPT → BIA 取得生物特征数据 <20>

BIA 从CD<请将手指放在光照板上>

用户将手指放在扫描器上

BIA → RPT 可以

RPT → BIA 取得Pin <40>

BIA 从CD:<请输入你的PIC,然后按<回车>>

个人输入PIC ， 然后<回车>

BIA → RPT 可以

RPT → BIA 取得帐号<40>

BIA 从CD: <现在输入你的帐户索引代码，然后按<回车>

个人输入代码，然后<回车>

BIA → RPT 可以

RPT → BIA 确认量值<452.33><40>

BIA 从CD: <量值 452.33 可以吗？>

个人输入可以

BIA → RPT 可以

RPT → BIA 赋值寄存器<1><123456>

BIA → RPT 可以

RPT 形成消息<交易>

BIA → RPT<交易请求消息>

BIA → RPT 可以

BIA 从CD: <我正在与DPC 中心通话>

RTP → DPC<交易请求消息>

DPC 确认生物特征数据，检索帐号→ 4024-2256-5521-1212

DPC → VISA<授权 4024-2256-5521-1212 452.33 123456>

VISA → DPC<可以 4024-2256-5521-1212 452.33 123456 授权代码>

DPC:取得专用代码

DPC → RPT<交易响应消息>

RPT → BIA 显示响应<交易响应消息><8>

BIA/LCD:<交易完成: 我被完全说服>

BIA → RPT<可以<授权代码>>

RPT: 打印带有授权代码的收据

1.6.2.国际互联网销售点终端

在该例中, IPT 与一个标准的 BIA 通信并且 DPC 授权一个交易。交易量为 452.33, 个人帐户为 4024-2256-5521-1212 , 国际互联网商户位于 merchant.com , 其商户代码为 123456 , 个人专用代码为“我被完全说服”。

IPT → merchant.com <如果资源允许请给我商户代码>

merchant.com → IPT<可以 123456 merchant.com 公共密钥>

IPT 产生对话密钥, 利用 merchant.com - 公共密钥加密

IPT → merchant.com <对话密钥>

与商户所有的随后的通信都利用对话密钥加密。

merchant.com → IPT<价格和产品信息>

IPT/屏幕: 显示价格和产品信息

个人: 选择项目“干果饼, 价格 45.33”

IPT → BIA 设置语言<英语>

BIA → IPT 可以

IPT → BIA 取得生物特征数据 <20>

BIA/LCD<请将手指放在光照板上>

用户将手指放在扫描器上

BIA → IPT 可以

IPT → BIA 取得 Pin<40>

BIA/LCD:<请输入你的 PIC,然后按<回车>>

个人输入代码, 然后按<回车>

BIA → IPT 可以

RPT → BIA 取得帐号<40>

BIA/LCD:<现在输入你的帐户索引代码，然后按<回车>

个人输入代码，然后按<回车>

BIA → IPT 可以

IPT → BIA 确认量值<45.33><40>

BIA/LCD:<量值 45.33 可以吗？>

个人输入可以

BIA → IPT 可以

IPT → BIA 赋值寄存器<1><123456>

BIA → IPT 可以

IPT → BIA 赋值寄存器<1><merchant.com>

BIA → IPT 可以

IPT → BIA 赋值寄存器<1><干果饼>

BIA → IPT 可以

IPT → BIA 形成消息<远程交易>

BIA → IPT<远程交易请求消息>

BIA → IPT 可以

BIA/LCD:<我正在与 DPC 中心通话>

IPT → merchant.com <远程交易请求消息>

merchant.com →安全利用 DPC 公共密钥连接到 DPC

merchant.com → DPC<远程交易请求消息>

DPC 确认生物特征数据，检索帐号→ 4024-2256-5521-1212

DPC 利用代码 123456 确认国际互联网 merchant.com

DPC → VISA<授权 4024-2256-5521-1212 45.33 123456>

VISA → DPC<可以 4024-2256-5521-1212 45.33 123456 授权码>

DPC:取得专用代码

DPC → merchant.com <交易响应消息>

merchant.com 存储授权代码

merchant.com → IPT<交易响应消息>

IPT → BIA 显示响应<交易响应消息><8>

BIA /LCD:<交易完成: 我被完全说服>

BIA → IPT<交易完成>

1.6.3.国际互联网出纳终端

在该例中, ITT 与标准 BIA 、 DPC 和银行国际互联网服务器通信, 执行例行和非例行主银行操作. 注意 DPC 不参与任何交易的实际验证, 而只负责生成一组有效的网络凭证并保证到银行的通信线路的安全。

ITT → bank.com <如果资源可用, 向我发送银行代码>

bank.com → ITT<可以 1200>

ITT → BIA 设置语言<英语>

BIA → ITT 可以

ITT → BIA 取得生物特征数据<20>

BIA /LCD<请将手指放在光照板上>

用户将手指放在扫描器上

BIA → ITT 可以

ITT → BIA 取得 Pin<40>

BIA /LCD:<请输入你的 PIC ,然后按<回车>>

个人输入 PIC, 然后按<回车>

BIA → ITT 可以

RPT → BIA 取得帐号<40>

BIA /LCD: <现在输入你的帐户索引代码, 然后按<回车>

个人输入代码, 然后按<回车>

BIA → ITT 可以

ITT → BIA 赋值寄存器<1><1200><银行代码>

BIA → ITT 可以

ITT → BIA 赋值寄存器<2><bank.com >

BIA → ITT 可以

ITT → BIA 赋值寄存器<3><ITT 端口,

bank.com 端口> (TCP/IP 地址)

BIA → ITT 可以

ITT →形成消息<网络凭证>

BIA → ITT<网络凭证请求>

BIA → ITT 可以

BIA/LCD:<我正在与DPC 中心通话>

ITT → DPC<网络凭证请求>

DPC: 确认生物特征数据，生成凭证（时间，帐户，银行）

DPC：取得专用代码

DPC → ITT<网络凭证请求>

ITT → BIA 显示响应<网络凭证响应>

BIA 解密响应，检查响应

BIA/LCD:<凭证可以：我被完全说服>

BIA 利用银行的公共密钥对凭证、对话密钥、
要求密钥进行加密

BIA → ITT<安全连接请求消息>

BIA → ITT<对话密钥>

BIA → ITT 可以

BIA/LCD:<进行到bank.com 的安全连接>

ITT → bank.com <安全连接请求消息>

bank.com 利用专用密钥解密，，确认凭证，使用共享密钥

bank.com → ITT<可以>

ITT → bank.com 连接的进一步交易都通过利用 ITT/银行对话密钥由 ITT 加密。

银行确定为非例行的任何交易必须由使用 BIA 的要求－响应机制的个人确认。

要求－响应机制只有当 BIA 处于“安全连接”状态才是可行的。

bank.com → ITT<确认<确认请求>>

ITT → BIA 确认私人信息<加密确认请求>

BIA 解密要求部分，并显示之

BIA/LCD:<请准许：将 12,420.00 转到 1023-3302-2101-1100>

用户输入可以

BIA 利用要求密钥重新加密响应

BIA /LCD: <进行到 bank.com 的安全连接>

BIA → ITT <可以<加密的确认响应>>

ITT → bank.com <加密的确认响应>>

1.6.4.电子签字终端

在该例中， EST 与一个标准的 BIA 和 DPC 通信以构成数字签字。个人专用代码

“我被完全说服”并且被签字的文件被称为“商品型号证”。

CET → BIA 设置语言<英语>

BIA → CET 可以

CET → BIA 取得生物特征数据<20>

BIA /LCD <请将手指放在光照板上>

用户将手指放在扫描器上

BIA → CET 可以

CET → BIA 取得 Pin<40>

BIA /LCD:<请输入你的 PIC,然后按<回车>>

用户输入 PIC，然后按<回车>

BIA → CET 可以

CET → BIA 确认文件<商品型号证><40>

BIA /LCD:<文件“商品型号证”可以吗?>

用户输入可以

BIA → CET 可以

CET → BIA 赋值寄存器<1><文件 MD5 值>

BIA → CET 可以

CET →形成消息<签字呈送>

BIA → CET<电子签字请求>

BIA → CET 可以

BIA /LCD: <我正在与 DPC 中心通话>

CET → DPC<电子签字请求>

DPC：确认生物特征数据，生成签字，返回签字文本代码

DPC：取得专用代码

DPC → CET<电子签字请求>

CET → BIA 显示响应<电子签字响应><8>

BIA/LCD:<文件完成：我被完全说服>

BIA → CET<可以<签字文本代码>>

1.6.5.验证的电子邮件终端

在该例中，CET 与一个标准的 BIA 和 DPC 通信以传输认证的电子邮件。个人专用代码为“我被完全说服”并且文件名为“上校舰长”。

CET → BIA 设置语言<英语>

BIA → CET 可以

CET → BIA 取得生物特征数据<20>

BIA/LCD<请将手指放在光照板上>

用户将手指放在扫描器上

BIA → CET 可以

CET → BIA 取得 Pin<40>

BIA/LCD:<请输入你的 PIC,然后按<回车>>

用户输入 PIC，然后按<回车>

BIA → CET 可以

CET → BIA 确认文件<上校舰长><40>

BIA/LCD:<文件“上校舰长”可以吗?>

用户输入可以

CET/屏幕：<接收方列表？>

用户输入<fred@ telerate.com joe@ reuters.com >

CET → BIA 赋值寄存器<1><fred@ telerate.com

joe@ reuters.com >

BIA → CET 可以

CET →形成消息<文件提交>

BIA → CET<电子文件提交请求>

BIA → CET 可以

BIA/LCD:<我正在与 DPC 中心通话>

CET → DPC<电子文件提交请求>

DPC: 确认生物特征数据，生成消息，返回消息#001234

DPC: 取得专用代码

DPC → CET<电子文件提交响应>

CET → BIA 显示响应<电子文件提交响应><8>

BIA/LCD:<文件完成: 我被完全说服>

BIA → CET<文件可以<1234>>

CET → DPC<电子文件数据请求，1234，部分 1，未完成>

DPC → CET<电子文件数据响应，未完成>

CET → DPC<电子文件数据请求，1234，部分 2，未完成>

DPC → CET<电子文件数据响应，未完成>

CET → DPC<电子文件数据请求，1234，部分 3，未完成>

DPC → CET<电子文件数据响应，未完成>

CET → DPC<电子文件数据请求，1234，部分 4，完成>

DPC → CET<电子文件数据响应，，跟踪 1234.1 1234.2>

DPC → fred@ telerate.com <电子邮件 1234.1 消息到达>

DPC → joe@ reuters.com <电子邮件 1234.2 消息到达>

mailer@ telerate.com → DPC<收到 1234.1 的通知电子邮件>

DPC → sender@ company.com <电子邮件 1234.1 接收方被通知>

mailer@ reuters.com → DPC<收到 1234.1 的通知电子邮件>

DPC → sender@ company.com <电子邮件 1234.1 接收方被通知>

[在 Fred 的 CET: Fred 存储“消息到达”电子邮件消息，并决定取出该消息]

CET → BIA 设置语言<英语>

BIA → CET 可以

CET → BIA 取得生物特征数据<20>

BIA /LCD<请将手指放在光照板上>

用户将手指放在扫描器上

BIA → CET 可以

CET → BIA 取得Pin<40>

BIA /LCD:<请输入你的PIC>

个人输入PIC，然后按<回车>

BIA → CET 可以

CET → BIA 赋值寄存器<1><1234.1>

BIA → CET 可以

CET → 形成消息<文件检索>

BIA → CET<电子文件检索请求>

BIA → CET 可以

BIA /LCD:<我正在与DPC 中心通话>

CET → DPC<电子文件检索请求>

DPC: 确认生物特征数据，查找1234.1

DPC： 取得专用代码

DPC → CET<电子文件检索响应>

CET → BIA 显示响应<电子文件检索响应><8>

BIA /LCD:<文件完成: 我被完全说服>

BIA → CET<文件可以<消息密钥>>

CET /屏幕: 解密，然后显示文件

1.6.6.安全传真终端

在该例中， SFT 与BIA /catv 和DPC 通信以传输安全传真。

SFT → BIA 取得生物特征数据<20>

BIA /LCD<请将手指放在光照板上>

用户将手指放在扫描器上

BIA → SFT 可以

BIA/LCD:<请输入你的PIC,然后按<回车>>

用户PIC，然后按<回车>

SFT → BIA 取得Pin<40>

BIA/LCD:<请输入你的职别索引，然后按<回车>>

用户输入职别索引，然后按<回车>

SFT → BIA 设置职别索引代码<40>

BIA → SFT 可以

SFT/屏幕: <接收方？（分机加*，末尾加#）>

用户输入<1 510 944-6300*525#)

SFT/屏幕: <接收方？（分机加*，末尾加#）>

用户输入<1 415-877-7770#)

SFT/屏幕: <接收方？（分机加*，末尾加#）>

用户输入<#>

SFT → BIA 赋值寄存器<1><15109446300*525 14158777770>

BIA → SFT 可以

SFT →形成消息<文件提交>

BIA → SFT<安全传真提交请求>

BIA → SFT 可以

BIA/LCD:<我正在与DPC 中心通话>

SFT → DPC<安全传真提交请求>

DPC: 确认生物特征数据，生成消息，返回消息#001234

DPC: 取得专用代码

DPC → SFT<安全传真提交响应>

SFT → BIA 显示响应<安全传真提交响应><10>

BIA/LCD:<文件完成: 我被完全说服>

BIA → SFT<文件可以<001234>>

SFT → DPC<安全传真数据请求，1234，部分1，未完成>

DPC → SFT<安全传真数据响应，未完成>

SFT → DPC<安全传真数据请求，1234，部分2，未完成>

DPC → SFT<安全传真数据响应，未完成>

SFT → DPC<安全传真数据请求，1234，部分 3，未完成>

DPC → SFT<安全传真数据响应，未完成>

SFT → DPC<安全传真数据请求，1234，部分 4，完成>

DPC → SFT<安全传真数据响应>

DPC →连接传真 15109446300

DPC → SFT6300<传真首页“Sam Spade”来自"Fred Jones"
1234.1 4 页等待>

DPC →断开

DPC →连接传真 14158777770

DPC → SFT7770<传真首页“John Jett”来自"Fred Jones"
1234.2 4 页等待>

DPC →断开

[在 Sam 的 SFT： Sam 看到来自 Fred 的传真首页，利用跟踪代码 1234.1 从 DPC 中检索文件。]

SFT → BIA 取得生物特征数据<20>

BIA /LCD<请将手指放在光照板上>

用户(Sam)将手指放在扫描器上

BIA → SFT 可以

SFT → BIA 取得 Pin<40>

BIA /LCD:<请输入你的 PIC，然后按<回车>>

用户(Sam)输入职别索引，然后按<回车>

BIA → SFT 可以

SFT → BIA 赋值寄存器<1><1234.1>

BIA → SFT 可以

SFT →形成消息<文件检索>

BIA → SFT<安全传真检索请求>

BIA → SFT 可以

BIA /LCD: <我正在与 DPC 中心通话>

SFT → DPC<安全传真检索请求>

DPC: 确认生物特征数据，查找1234.1,验证生物特征数据—
PIC=Sam Spade

DPC: 在数据库中查找专用代码

DPC → SFT<安全传真检索响应>

SFT → BIA 显示响应<安全传真检索响应><8>

BIA → SFT<文件可以:我被完全说服<消息密钥>>

SFT/屏幕: <文件可以:我被完全说服>

SFT/屏幕: 打印传真

1.6.7.生物特征数据登记终端

在该例中，BRT 与一个登记BIA 和DPC 通信以在系统中登记用户。

BRT → BIA 设置语言<英语>

BIA → BRT 可以

BRT → BIA 取得生物特征数据<20><主要>

BIA/LCD<请将主手指放在光照板上>

用户将主手指放在扫描器上

BIA → BRT 可以

BRT → BIA 取得生物特征数据<20><辅>

BIA/LCD<请将辅手指放在光照板上>

用户将辅手指放在扫描器上

BIA → BRT 可以

SFT → BIA 取得Pin<40>

BIA/LCD:<请输入你的PIC，然后按<回车>>

用户输入123456，然后按<回车>

BIA → BRT 可以

BRT → BIA 取得消息密钥

BIA → BRT<可以<消息密钥>>

BIA →<登记请求消息>

BRT /屏幕: <名字:>

代表输入<R red G . Shultz>

BRT /屏幕: <地址:>

代表输入<1234 North Main>

BRT /屏幕: <邮政编码:>

代表输入<94042>

BRT /屏幕: <专用代码:>

代表询问个人，然后输入<我被完全说服>

BRT /屏幕: <资产帐户列表: >

代表输入<2,1001-2001-1020-2011> (信用卡)

代表输入<3,1001-1002-0039-2212> (支票帐户)

BRT /屏幕: <紧急帐户>

代表输入 <1,1001-1002-0039-2212> (紧急，支票帐户)

BRT → 形成消息<登记>

BIA → BRT<登记请求消息>

BIA → BRT 可以

BIA /LCD: <我正在与DPC 中心通话>

BRT 向请求中附加消息-密钥-加密的个人信息

BRT → DPC 登记请求消息<加密的个人信息>

DPC: 确认PIC 123456

DPC → BRT<登记响应消息>

BRT → BIA 显示响应<登记响应消息><8>

BIA /LCD<登记完成:我被完全说服，123456>

BIA → BRT<可以>

1.6.8.客户服务终端

在该例中，CST 与一个标准的BIA 和DPC 通信以验证个人的身份和凭证。

CST → BIA 设置语言<英语>

BIA → CST 可以

CST → BIA 取得生物特征数据<20>

BIA 从 CD <请将手指放在光照板上>

用户将手指放在扫描器上

BIA → CST 可以

CST → BIA 取得 Pin<40>

BIA 从 CD:<请输入你的 PIC，然后按<回车>>

用户输入 PIC，然后按<回车>

BIA → CST 可以

CST → BIA 取得消息密钥

BIA → CST<可以<消息密钥>>

CST → 形成消息<用户识别请求>

BIA → CST<用户识别请求>

BIA → CST 可以

BIA 从 CD:<我正在与 DPC 中心通话>

CST → DPC<用户识别请求>

DPC: 取得专用代码，个人特权

DPC → CST<用户识别应答>

CST → BIA 显示响应<用户识别应答><8>

BIA 从 CD <识别完成:我被完全说服>

BIA → CST<可以<个人名称特权>>

CST: 检验特权，看是否足以供 CST 使用

1.6.9 发行人终端

在该例中，IT 与一个标准的 BIA 和 DPC 通信以授权并向 DPC 发送一组帐户增加和删除请求。个人专用代码为“我已被完全说服”，银行代码为 1200。

IT → BIA 设置语言<英语>

BIA → IT 可以

IT → BIA 取得生物特征数据<20>

BIA /LCD<请将手指放在光照板上>

用户将手指放在扫描器上

BIA → IT 可以

IT → BIA 取得Pin<40>

BIA /LCD:<请输入你的PIC，然后按<回车>>

用户输入PIC，然后按<回车>

BIA → IT 可以

IT → BIA 赋值寄存器<1><1200>

BIA → IT 可以

IT → BIA 取得消息密钥

BIA → IT <消息密钥>>

BIA → IT 可以

IT → BTA 形成消息<发行人请求>

BIA → IT<发行人批处理请求>

BIA → IT 可以

BIA /LCD:<我正在与DPC 中心通话>

IT → DPC<发行人批处理请求><由消息密钥加密的发行人批处理>

DPC：确认生物特征数据，确认银行代码1200与BIA 标识

DPC：取得专用代码

DPC：利用消息密钥解密，执行发行人批处理

DPC → IT<发行人批处理应答>

IT → BIA 显示响应<发行人批处理应答><8>

BIA /LCD<批处理完成:我被完全说服>

BIA → IT<可以>

1.6.10.自动出纳机

在该例中，ATM 与一个集成ATM BIA 和DPC 通信，以识别用户并获得他的银行帐号。用户帐号为2100-0245-3778-1201,银行代码为2100,用户专用代码为“我已被完全说服”。

ATM → BIA 取得生物特征数据<20>

ATM 从LCD<请将手指放在光照板上>

用户将手指放在扫描器上

BIA → ATM 可以

ATM 从LCD:<请输入你的PIC，然后按<回车>>

用户在ATM 键盘上输入123456，然后按<回车>

ATM → BIA 设置Pin<123456>

BIA → ATM 可以

ATM 从LCD:<现在输入你的帐户索引代码，然后按<回车>>

用户输入2，然后<回车>

ATM → BIA 设置帐户索引代码<2>

BIA → ATM 可以

ATM → BIA 赋值寄存器<1><2100>

BIA → ATM 可以

ATM → 形成消息<帐户访问>

BIA → ATM <帐户访问请求消息>

BIA → ATM 可以

ATM 从LCD:<我正在与DPC 中心通话>

ATM → DPC<帐户访问请求消息>

DPC：确认生物特征数据，检索帐号→ 2100-0245-3778-1201

DPC：取得专用代码

DPC → ATM <帐户访问响应消息>

ATM → BIA 解密响应<帐户访问响应消息>

BIA → ATM <2100-0245-3778-1201><无紧急><我已被完全说服>

ATM 从LCD<我已被完全说服>

此时，ATM 具有了其继续进行所需的帐号，所以它然后检索与该帐号相关的信息，并与用户进行交互作用。

1.6.11.电话销售点终端

在该例中， PPT 与一个集成的电话 BIA 和电话商户通信，利用电话安全地下载信息和购买物品。用户 PIC 为 1234，帐户索引代码为 1，商户电话号码为 1 800 542-2231，商户代码 123456，实际帐号为 4204-2256-5521-1212 。

注意电话在将电话号码置入系统之前去掉区号（ 1-800 ）。

用户拨打电话 18005422231

PPT →连接商户 18005422231

PPT → BIA 赋值寄存器 1<5422231>

销售代表应答。用户选择项目“干果饼”。

销售代表下载信息

商户→ PPT<123456 干果饼 43.54>

PPT → BIA 取得生物特征数据<20>

电话/LCD： <请将手指放在光照板上>

用户将手指放在扫描器上

BIA → PPT 可以

电话/LCD:<请输入你的 PIC ， 然后按#>

用户在键盘上输入 1234， 然后按#或者*（回车）

PPT → BIA 设置 Pin<1234>

BIA → PPT 可以

电话/LCD:<现在输入你的帐户索引代码>

用户输入 1， 然后<回车>

RPT → BIA 设置帐户索引代码<1>

BIA → PPT 可以

PPT → BIA 赋值寄存器<2><123456>

BIA → PPT 可以

电话/LCD:<如果 45.54 可以的话按#>

用户输入#（是）

PPT → BIA 设置数量<45.54>

BIA → PPT 可以

PPT →形成消息<远程交易>

BIA → PPT<远程交易请求>

BIA → PPT 可以

电话/LCD:<我正在与 DPC 中心通话>

PPT →商户<电话交易请求>

商户→ DPC: 利用 DPC 公共密钥安全连接到 DPC

商户→ DPC<电话交易请求>

DPC: 确认生物特征数据, 检索帐号→ 4024-2256-5521-1212

DPC: 确认商户 5422231 具有代码 123456

DPC → VISA<授权 4024-2256-5521-1212 43.54 123456>

VISA → DPC<可以 4024-2256-5512-1212 43.54 123456 授权代码>

DPC: 取得专用代码

DPC →商户<交易请求消息>

商户检验响应代码

商户→ PPT<交易响应消息>

PPT → BIA 解密消息<交易响应消息>

BIA → PPT<可以<我已被完全说服><授权代码>>

电话/LCD: <鸣音>交易完成: 我已被完全说服

1.6.12.有线电视销售点终端

在该例中, CPT 与集成有线电视 BIA 和有线电视商户通信,利用有线电视广播网络安全地下载信息和购买物品. 用户 PIC 为 1234, 帐户索引代码为 1, 频道为 5, 商户代码为 123456, 实际帐号为 4024-2256-5521-1212.

用户将电视调谐到 5 频道.

商户→ CPT<干果饼 43.54 123456> (广播)

用户在电视遥控器上击中“买”

CPT/TV: <买价格为$43.54 的干果饼>

CPT → BIA 取得生物特征数据<20>

CPY/TV：<请将手指放在光照板上>

用户将手指放在扫描器上

BIA → CPT 可以

CPT/TV:<请输入你的PIC，然后按#>>

用户在键盘上输入1234，然后按“买”

CPT → BIA 设置Pin<1234>

BIA → CPT 可以

CPT/TV:<现在输入你的帐户索引代码>

用户输入1，然后<回车>

RPT → BIA 设置帐户索引代码<1>

BIA → CPT 可以

RPT → BIA 赋值寄存器<1><频道5，15:30:20 PST>

BIA → RPT 可以

CPT → BIA 赋值寄存器<2><123456>

BIA → CPT 可以

CPT/TV:<如果45.54可以的话按“买”>

用户输入“买”

CPT → BIA 设置数量<43.54>

BIA → CPT 可以

CPT → 形成消息<有线电视交易>

BIA → CPT<有线电视交易请求>

BIA → CPT 可以

CPT/TV:<我正在与DPC 中心通话>

CPT → CTV 中心<有线电视交易请求>

商户→ DPC：利用DPC 公共密钥安全连接到DPC

商户→ DPC<有线电视交易请求>

DPC：确认生物特征数据，检索帐号→ 4024-2256-5521-1212

DPC：确认商户频道5,目前的节目代码为123456

DPC → VISA<授权4024-2256-5521-1212 43.54 123456>

VISA → DPC<可以 4024-2256-5512-1212 43.54 123456 授权代码>

DPC：取得专用代码，邮件地址

DPC →商户<交易响应消息>

商户检验响应代码，记录邮件地址

商户→ CTV 中心<交易响应消息>

CTV 中心→ CPT<交易响应消息>

CPT → BIA 解密消息<交易响应消息>

BIA → CPT<可以<我已被完全说服>授权代码>>

CPT/TV：<鸣音>交易完成：我已被完全说服

从上面所述可以看出，本发明的目的和特征是如何实现的。

第一，本发明提供了一个计算机识别系统，使用者不再需要拥有或者出示可以启动系统接受请求的实际的物品例如代价券。

第二、本发明提供了一种计算机识别系统，该系统可以验证使用者的身份，而无需验证要拥有某种专用物品及信息。

第三、本发明基于一个或者多个只与使用者物理上相关的唯一的特征来验证使用者的身份。

第四、本发明提供了一种实用的、方便的和容易使用的识别系统。

第五、本发明提供了一种可以安全接入到计算机系统，可以高度防止未经授权的使用者欺骗性的进入企图的系统。

第六、本发明提供一种计算机识别系统，可以使使用者通知授权方某个特定的访问请求是被第三方强制的，而第三方却不知道。

第七、本发明提供了一种识别系统，允许对电子消息和/或传真的发送方和接收方进行识别。

尽管本发明是针对特定的无代价券识别系统及其方法的，应当理解，在不背离后面所附的权利要求所限定的本发明的精神和范围的情况下可以对本发明作出各种改进和修改。

5.词汇表

帐户索引代码：与特定金融资产帐户相应的数字或字母数字序列。

AID：授权个人数据库：含有被授权使用个人和发行人BIA设备的个人的列表。

AOD：设备拥有者数据库：含有与每个BIA的拥有者有关的地理和联系信息的中央库。

ACSII：美国信息交换标准代码。

ATM：自动出纳机；使用编码的生物特征身份信息获得对金融资产管理系统的访问，包括取款和帐户管理。

BIA：生物特征输入装置；采集生物特征身份信息，对其编码和加密，使其可用于授权。有不同的硬件模型和软件版本。

生物特征：系统对个人自然人的某些方面的测量值。

生物特征ID：系统所用的标识符，以便唯一地标识个人的生物特征记录（IR ID－个人记录ID）。

BIO－PIC组：与相同个人标识代码链接的算法上不同的生物特征采样的集合。

BRT：生物特征登记终端；位于零售银行分支机构，BRT将生物登记信息与个人所选的PIN以及所选的个人信息结合起来，以将个人登记到系统中。

CBC：密码块链接：DES的一种加密模式。

CCD：电荷耦合器件。

CET：验证Email终端；利用BIA验证发送方，对文件加密，向系统传送。系统保存，向接收方通知系统收到消息。接收方标识自身，然后向接收方传送文件。一旦发送文件，向传送方通知。文件由BIA加密得以验证发送、保密。传送方可以请求传送状态。双方必须都是系统成员。

命令：驻留在DPC中的程序或例程，执行特定的任务，由发自装有BIA的终端的请求消息激活。

合同接受/拒绝：个人借以输入其BIO－PIC并执示DPC对已经利用电子传真发送给所述个人的文件中所含的术语的所述个人合同接受或拒绝进行登记的过程。

CPT：有线电视销售点终端：将向电视顶置盒指明产品信息的屏幕显示同播数字信号与产品影象以及利用CATV 通信网络执行生物特征－PIN 验证的BIA 远程控制器结合起来。定单/授权/邮件地址/商品ID 送到商户。授权结果显示在电视上。

CST：客户服务终端；向系统客户服务人员提供不同程度（根据访问权限）的访问能力，检索和修改个人信息，以便人们解决帐户问题。

数据密封步骤：结合消息的加密检查和，将明文转换为密文（称为“加密”），加密检查和允许以明文形式保存信息同时提供检测对消息的任何后续修改的装置。

DES：数字加密标准：对数字数据的密码保护的标准。见标准ANSI X 3.92-1981。

确定：在执行步骤中所处理的命令的状态。

DPC：数据处理中心，即为支持多个吉字节生物特征身份数据库的硬件、软件和人员所处的地点和单位。DPC 对电子消息进行处理，多数消息涉及作为前身执行生物特征身份检查，以执行某些动作，比如金融汇兑，或者发送传真，或者发送电子邮件，等等。

DSP：数字信号处理器：一种专用于信号处理应用所需的数学运算的集成电路。

DUKPT：每个交易的导出的唯一密钥：见标准ANSI/ABA X9.24-1992.

EDD：电子文件数据库：含有等待个人收取的所有悬置传真和电子消息的中央库。

紧急帐户索引：由个人选取的字母数字数位或序列，当被访问时，将导致系统将一个交易标定为紧急交易，可能造成显示假屏幕和/或向授权机关通知所述个人已被强制执行一次传输或交易。

ESD：电子签字数据库：含有任何人所签字的由授权号码指定的所有文件的所有MD5 和电子签字的中央库。

EST：电子签字终端：利用BIA 标识个人，计算机计算文件的检查和，将检查和发送到系统，系统对检查和进行验证、加时间标记、保存，并返回sig 代码．利用国际互联网（Internet）作为传送工具。EST 也

对所给签字验证 sig 代码和 MD5 计算。

FAR （错误接受率）：将一个个人的生物特征数据错误地标识为另一个个人的生物特征数据的统计似然性。

假屏幕：对已被有意预先确定为稍微不精确的信息的显示，使得强制方将不能非法获得与个人金融资产有关的精确数据，同时不注意对该信息的变更。

FDDI：光纤数字设备接口：利用光纤令牌环的网络设备。

FS：字段分隔符。

FW：防火墙机器：对进入和离开 DPC 的通信进行管理的国际互联网－局域网路由器。

GM：网关机器：DPC 中的主处理计算机；运行多数软件。

IBD：个人生物特征数据库：生物特征数据、金融资产及其他个人信息的中央库。利用对生物特征数据库的询问为交易授权和传输验证身份。

ID：发行人数据库：含有被允许向系统增加和删除金融资产帐户号码的机构的中央库。

IML：IBD 机器列表：DPC 中的软件模块，确定哪个 IBD 机器负责哪个 PIN 代码。

国际互联网商户：利用国际互联网（Internet）电子网络向消费者销售服务或货物的零售帐户。

IPT：国际互联网销售点终端：来自国际互联网的表项和商户代码，用于验证的 BIA 生物特征－PIN，利用国际互联网发送到系统，向商户传送授权/定单/PO 号。系统也利用国际互联网进行响应，在屏幕上显示结果。

发行人：将登记到 DPC 的金融资产的金融帐户发行人。

发行人批处理："增加"和"删除"指令集合，这些指令利用生物特征 ID、金融资产帐户以及由发行人向 DPC 提供的并经验证的帐户索引代码得以完成。

IT：发行人终端；向系统提供一批连接，以便发行人增加或从特定个人 IBD 记录上去除（他们的）金融资产帐户号码。

ITT：国际互联网出纳终端；利用加密的凭证对网络终端对话进行授权，凭证是利用生物特征ID从DPC获得的。

LCD：液晶显示（器）：一种用于显示文本的技术。

MAC：消息授权代码：一种加密的检查和算法，MAC提供一种保证：消息的内容在MAC计算之后不被更改。见标准ANSIX9.9-1986。

MACM：消息授权代码模块：DPC中的一种软件模块，它处理MAC验证并产生入站和出站包。

MDM：消息解密模块：DPC中的一种软件模块，它来自或发向BIA设备的包进行加密和解密。

MPM：消息处理模块：DPC中的一种软件模块，它执行对请求包的处理。

网络凭证：个人和银行都由DPC进行识别，以建立网络凭证。该凭证包括个人标识以及连接的内容（即，TCP/IP源和目的端口）。DPC利用个人帐户id、日时间以及银行代码建立网络凭证。DPC利用公共密钥加密和DPC的专用密钥对该凭证进行签字。

PFD：先前欺诈数据库：已与先前欺诈关联的IBD记录的中央库。对于每个新客户的生物特征数据对所有PFD记录进行检查，以便减少再次欺诈。

PGL：PIN组列表：DPC中的一种软件模块，用于维护IBD机器的结构。

PIN：个人识别号码，一种利用保密知识对个人帐户的访问进行保护的方法，由至少一个号码构成。

PIC：个人识别代码；由数字、符号或字母符号构成的PIN。

POS：销售点；货物售出的地点。

PPT：电话销售点终端：将电话号码与商品价格以及产品信息结合起来，以便在装有BIA的电话上对交易进行授权。定单/授权/邮件地址/PO被传送到商户。得到的授权与个人的专用代码一起显示在电话LCD上，或“讲出”。

RAM：随机存取存储器。

RF：射频：一般指在正常操作电气设备时所发射的射频能量。

寄存器：为特定目的、设置在芯片上的数据以及为指令所存储的操作数而保留的存储器。

请求：由BIA到DPC的电子指令，指示DPC验证个人并且从而在验证成功时对个人的命令进行处理。

RMD：远程商户数据库：含有对于商户电话和有线电视定购商店的所有商户识别代码；利用商户ID加索引。也含有每个商户系统加密代码。

RPT：零售销售点终端；将编码的生物特征身份信息与零售交易（信息可能来自电子现金出纳机）结合起来，并且利用X.25网络、调制调调器等提出系统的授权请求。

安全交易：其中至少一方已由DPC验证的电子消息或传真。

SFT：安全传真终端；采用BIA验证发送方，发送或者是非安全、发送方安全、安全、或者是安全－保密传真。后两者需要接收方利用生物特征PIN验证自身。利用（根据职别索引数字指定的）“职别”标记出站传真。发送方可以询问传送状态。参加双方必须是系统成员。发送方或者接收方能够请求将传真建档。

SNM：序列号码模块：DPC中的一种软件，它对入站请求包管理DUKPT序列号码。序列号码处理防止再次袭击。

终端：一种利用BIA收集生物特征采样并形成随之送到DPC用于授权和执行的请求消息的设备。终端几乎总是辅助地将信息加到请求消息上，指明对方等。

职别索引代码：唯一标识个人在其工作环境中得到授权的作用或能力的字母数字序列。

代价券：给定一种能力的无生命的物体。

跟踪代码：赋给存储在DPC中的或由之传送的数据的字母数字序列，使得可以利用所述序列检索该数据，或者获得与数据传输状态有关的报告。

交易：电子金融交换。

传输：除了电子金融交换之外的电子消息。

VAD：有效设备数据库：每个BIA在其中（与唯一加密代码关联）与该BIA的拥有者一起得以识别的中央库。

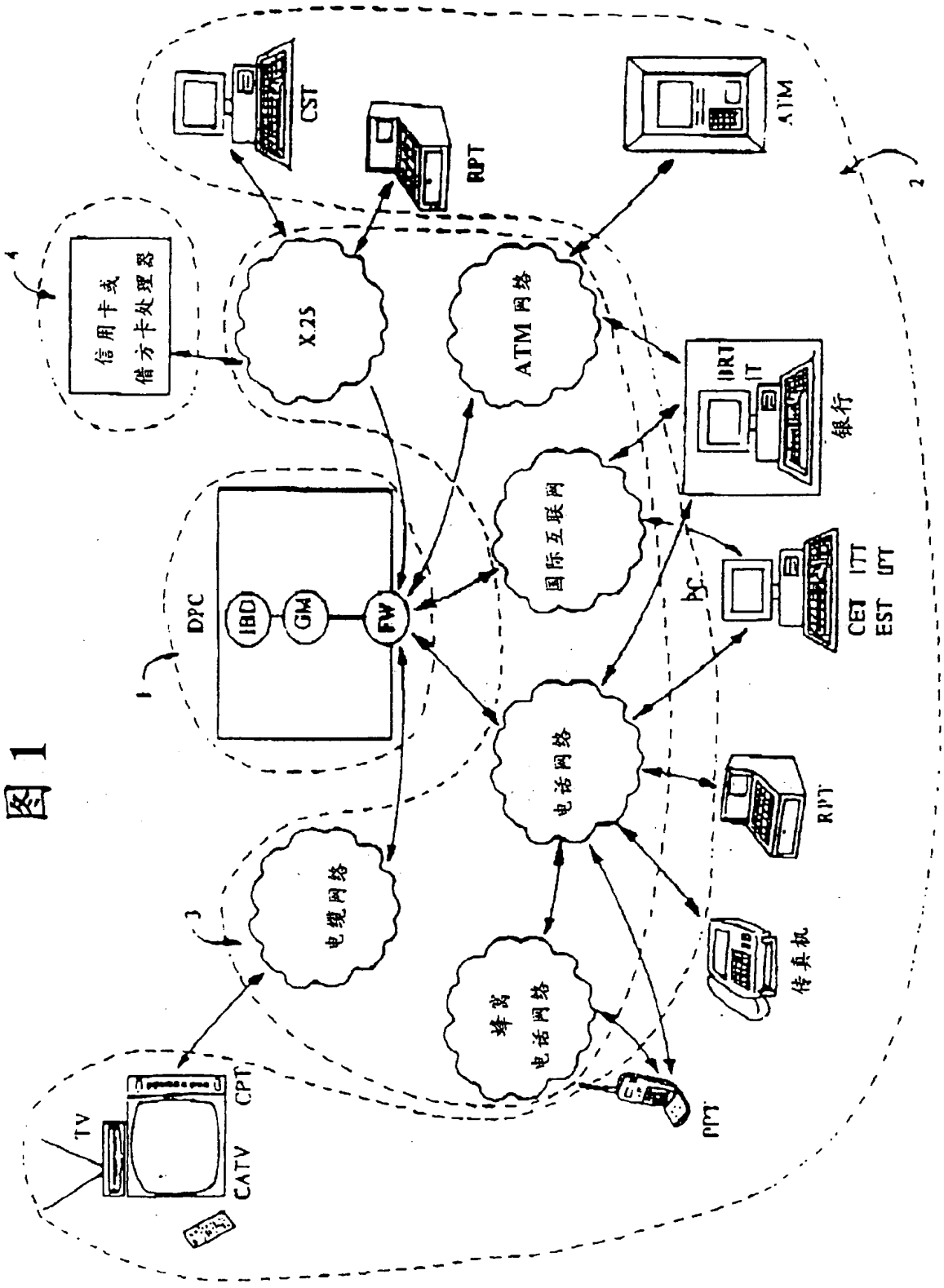
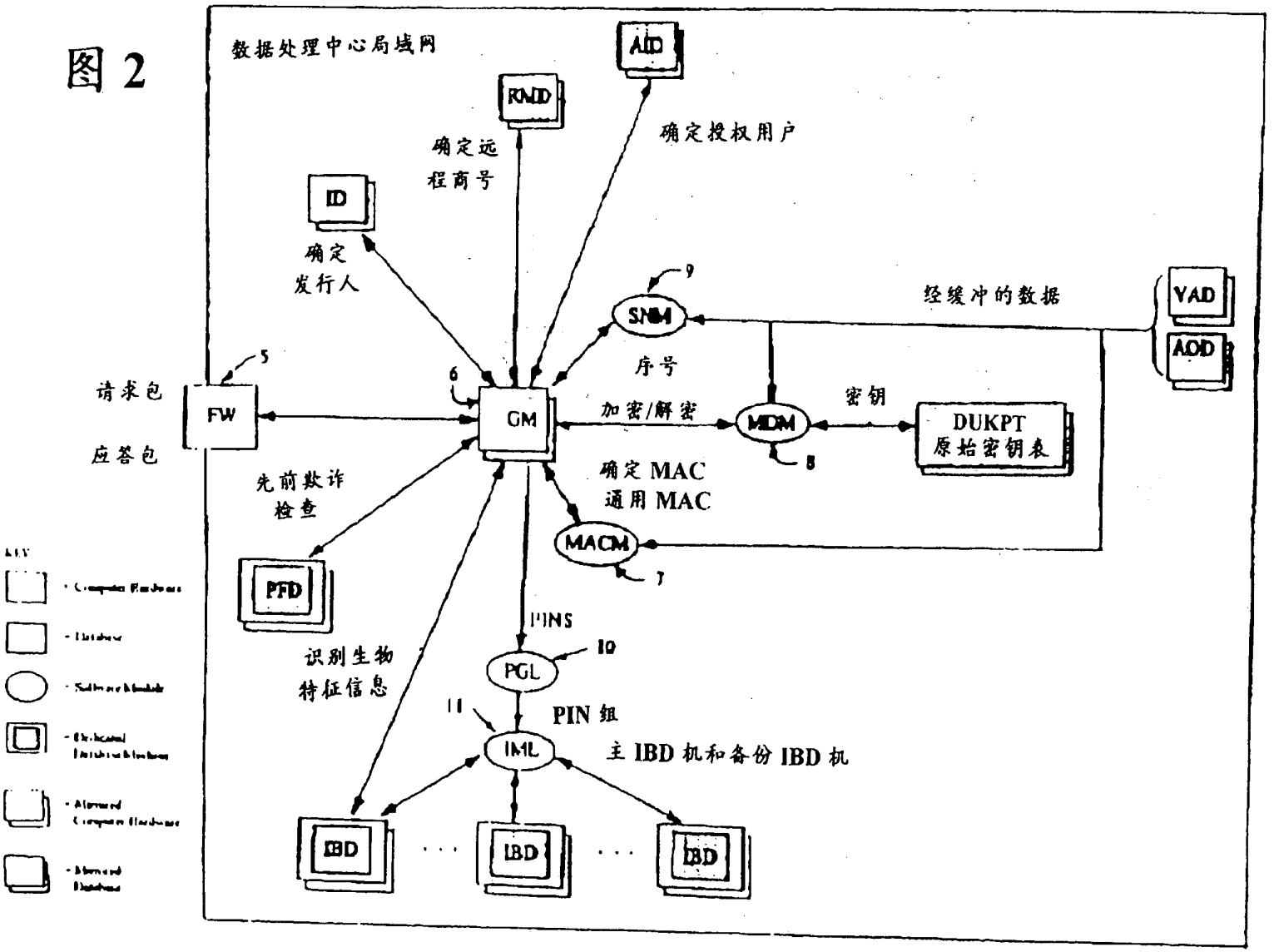

CST
RPT
ATM
信用卡或
借方卡处理器
X25
ATM 网络
IBRT
IT
银行
DPC
IBD
GM
FW
国际互联网
CET ITT
EST DT
电话网络
RPT
电缆网络
传真机
蜂窝
电话网络
PPT
TV
CATV
CPT

图 1

图 2


数据处理中心局域网
AID
RNID
确定远
程商号
确定授权用户
ID
确定
发行人
9
SNM
经缓冲的数据
YAD
AOD
序号
5
请求包
6
FW
GM
加密/解密
MDM
密钥
DUKPT
原始密钥表
8
应答包
确定 MAC
通用 MAC
先前欺诈
检查
MACM
7
PFD
PINS
识别生物
特征信息
10
PGL
11
PIN 组
IML
主 IBD 机和备份 IBD 机
IBD
IBD
IBD

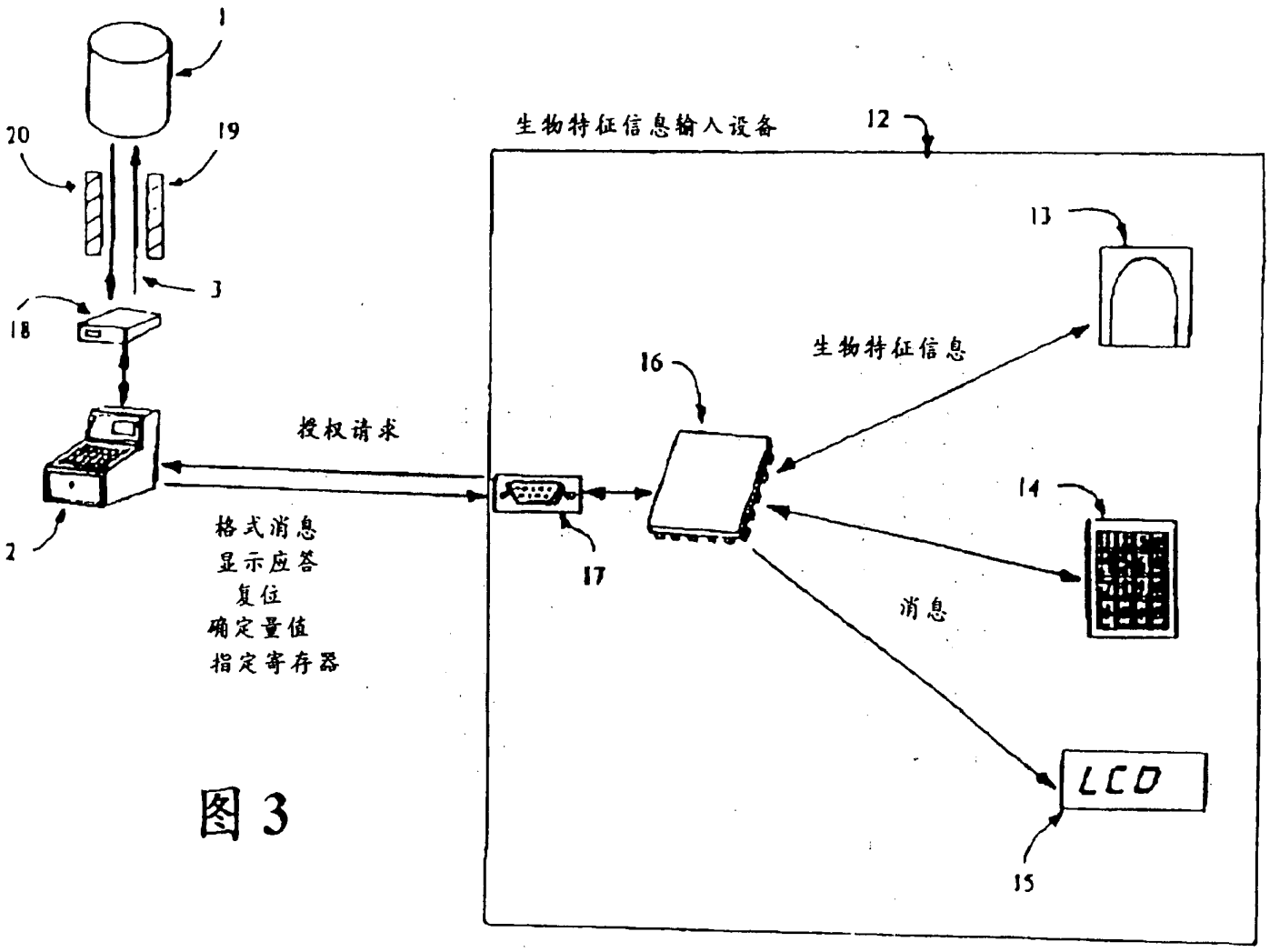

1
20
19
3
18
2
授权请求
格式消息
显示应答
复位
确定量值
指定寄存器
生物特征信息输入设备
12
13
生物特征信息
16
14
17
消息
LCD
15

图 3

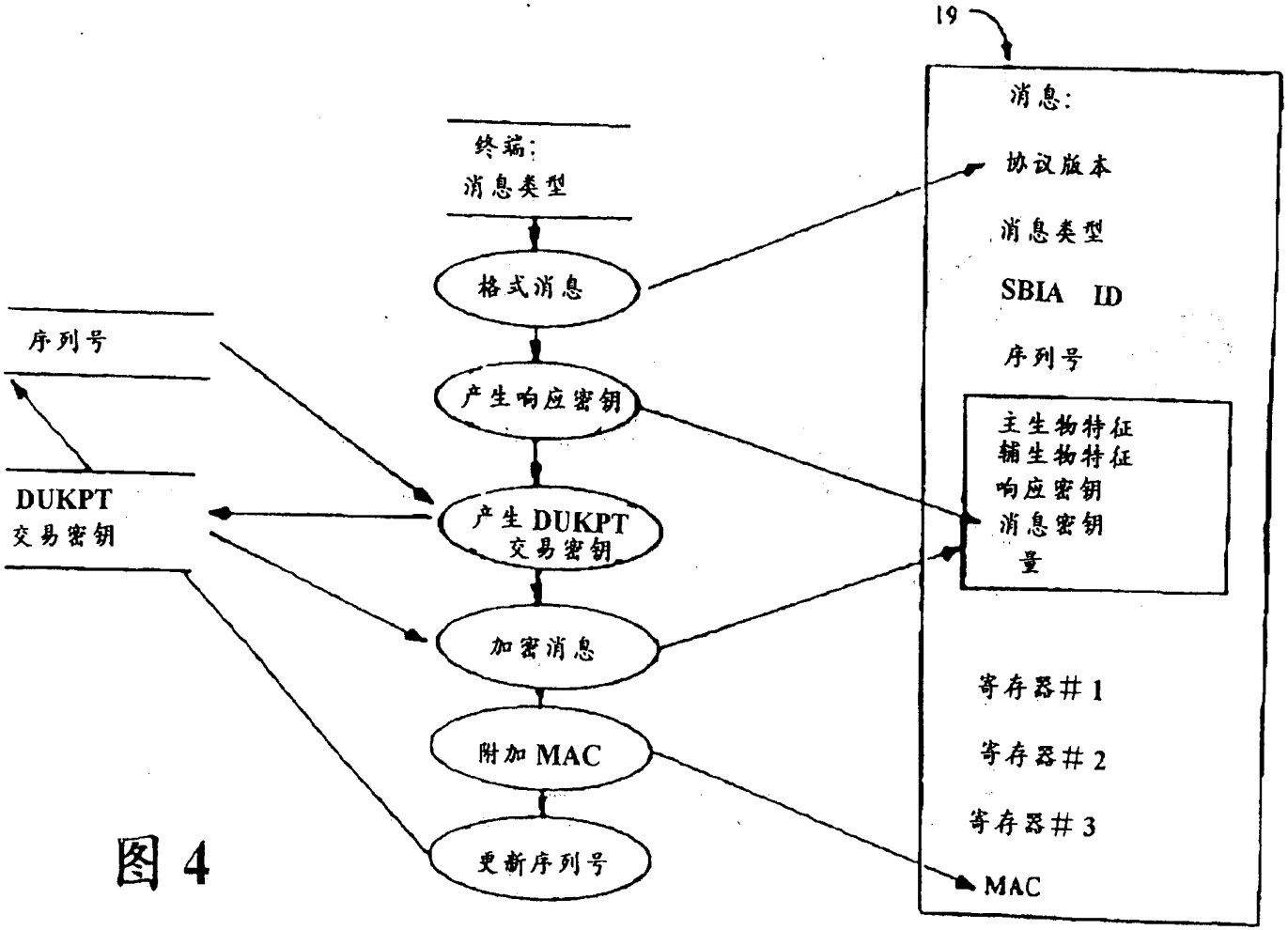

19
消息:
协议版本
消息类型
SBIA ID
序列号
主生物特征
辅生物特征
响应密钥
消息密钥
量
寄存器#1
寄存器#2
寄存器#3
MAC
终端:
消息类型
格式消息
产生响应密钥
产生 DUKPT
交易密钥
加密消息
附加 MAC
更新序列号
序列号
DUKPT
交易密钥

图 4

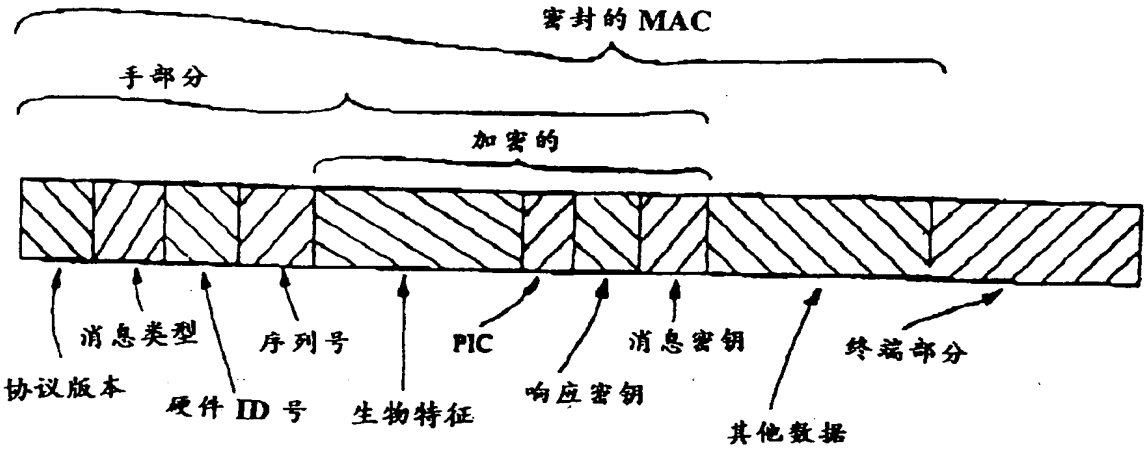

密封的 MAC
手部分
加密的
协议版本
消息类型
硬件 ID 号
序列号
生物特征
PIC
响应密钥
消息密钥
其他数据
终端部分

图 5

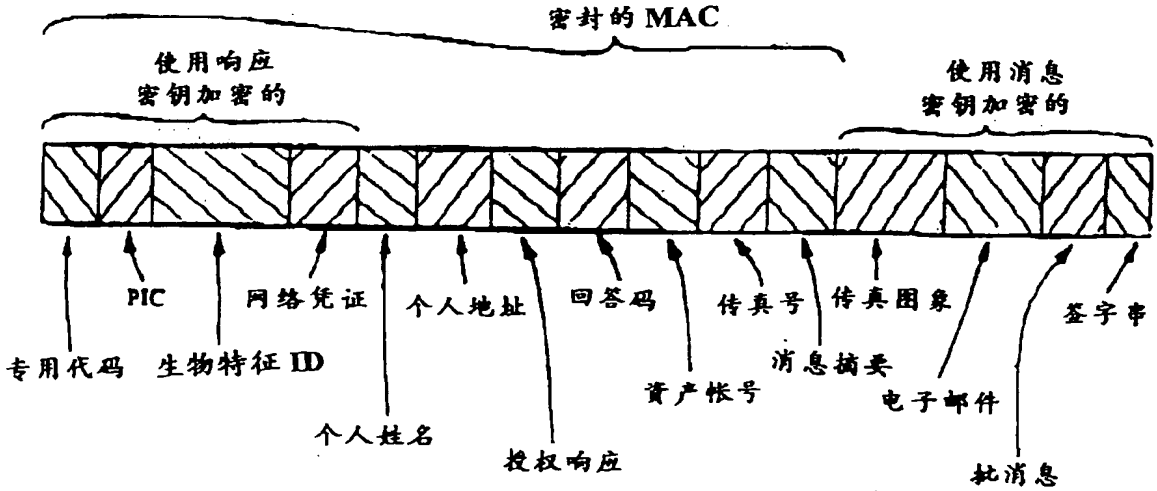

密封的 MAC
使用响应
密钥加密的
使用消息
密钥加密的
专用代码
PIC
生物特征 ID
网络凭证
个人姓名
个人地址
投权响应
回答码
资产帐号
传真号
消息摘要
传真图象
电子邮件
批消息
签字串

图 6

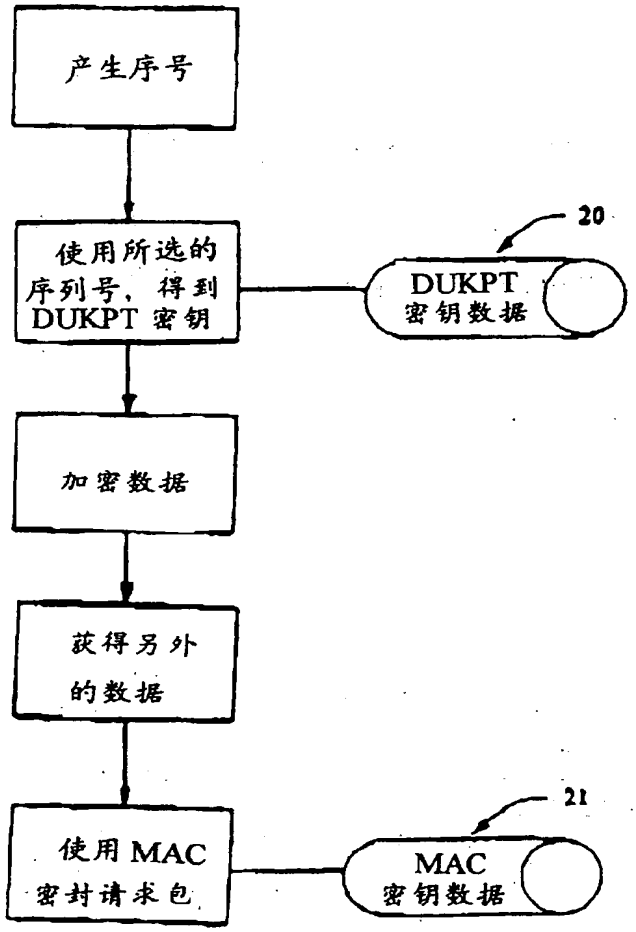

产生序号
使用所选的序列号，得到DUKPT密钥
20
DUKPT密钥数据
加密数据
获得另外的数据
使用MAC密封请求包
21
MAC密钥数据

图 7

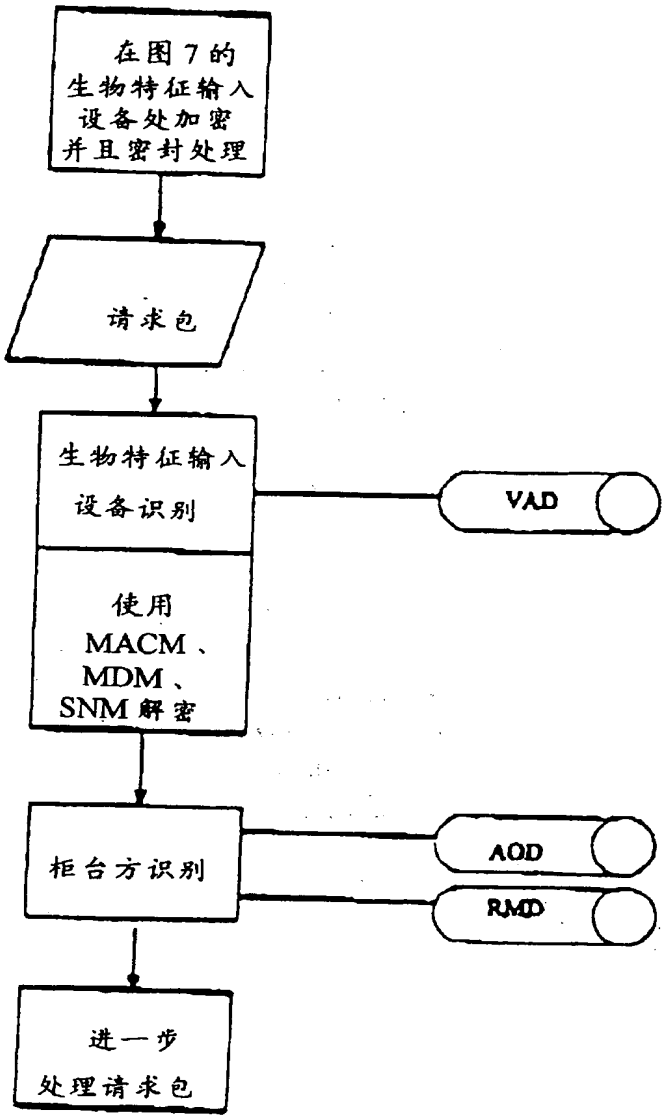

在图7的
生物特征输入
设备处加密
并且密封处理
请求包
生物特征输入
设备识别
VAD
使用
MACM、
MDM、
SNM解密
柜台方识别
AOD
RMD
进一步
处理请求包

图 8

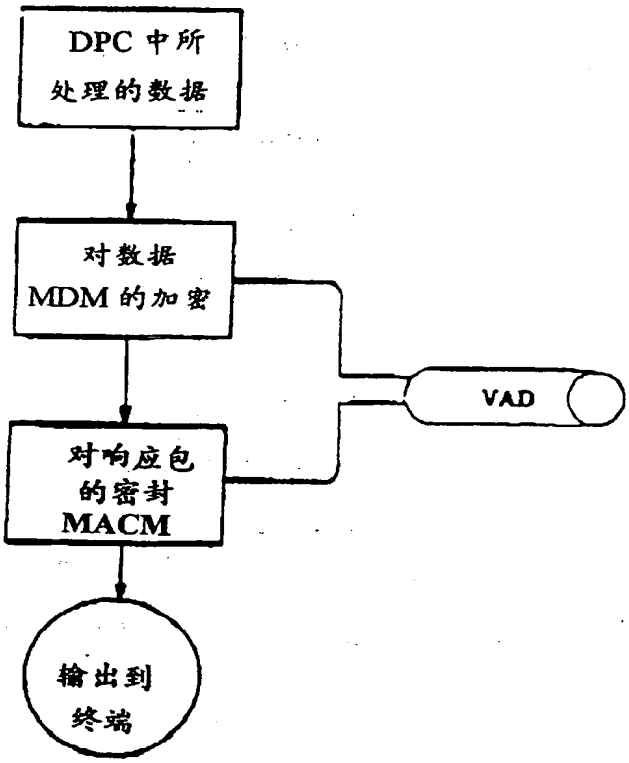


图 9

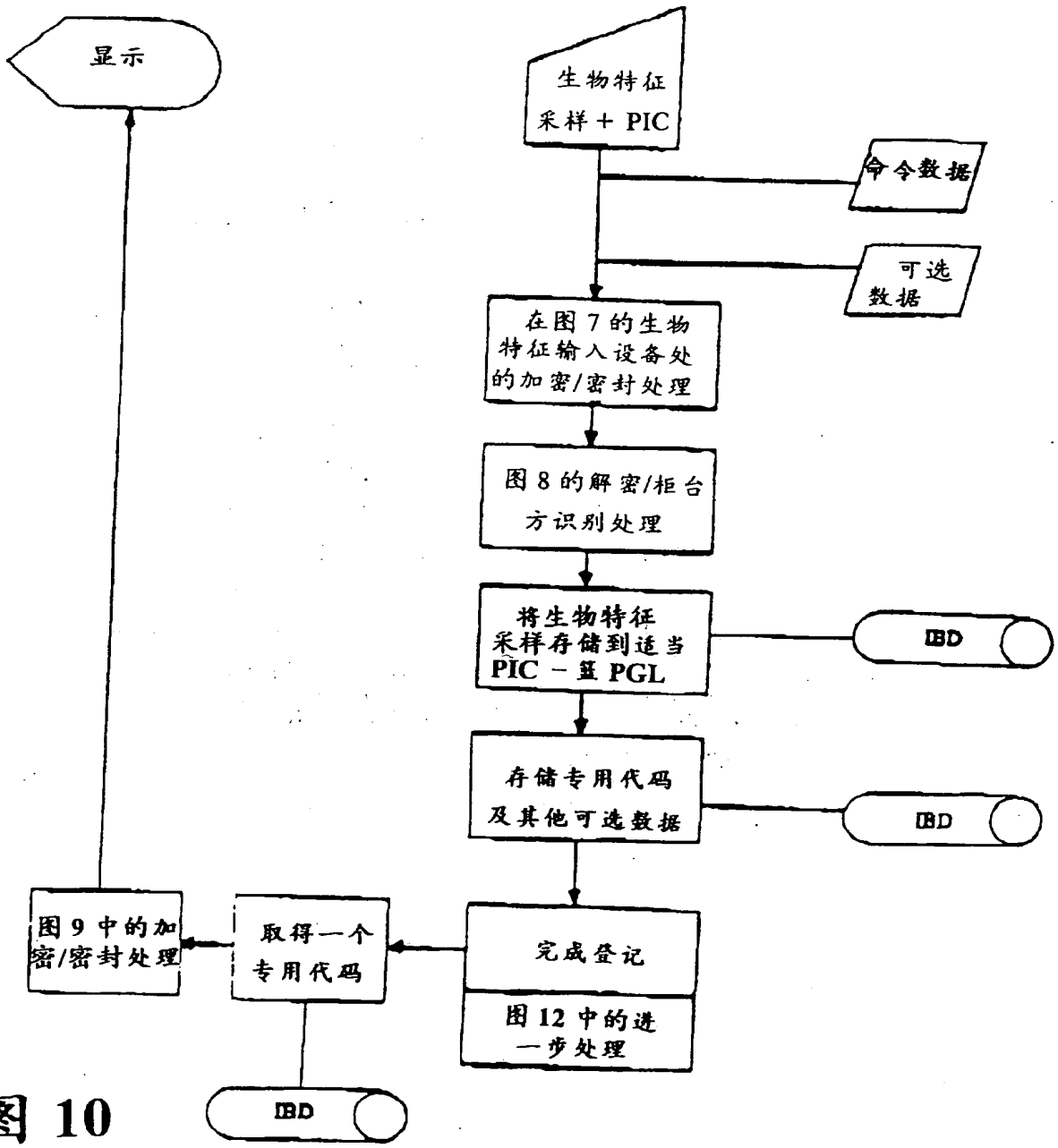

显示
生物特征
采样 + PIC
命令数据
可选
数据
在图 7 的生物
特征输入设备处
的加密/密封处理
图 8 的解密/柜台
方识别处理
将生物特征
采样存储到适当
PIC - 筐 PGL
DBD
存储专用代码
及其他可选数据
DBD
完成登记
图 12 中的进
一步处理
取得一个
专用代码
图 9 中的加
密/密封处理
DBD

图 10

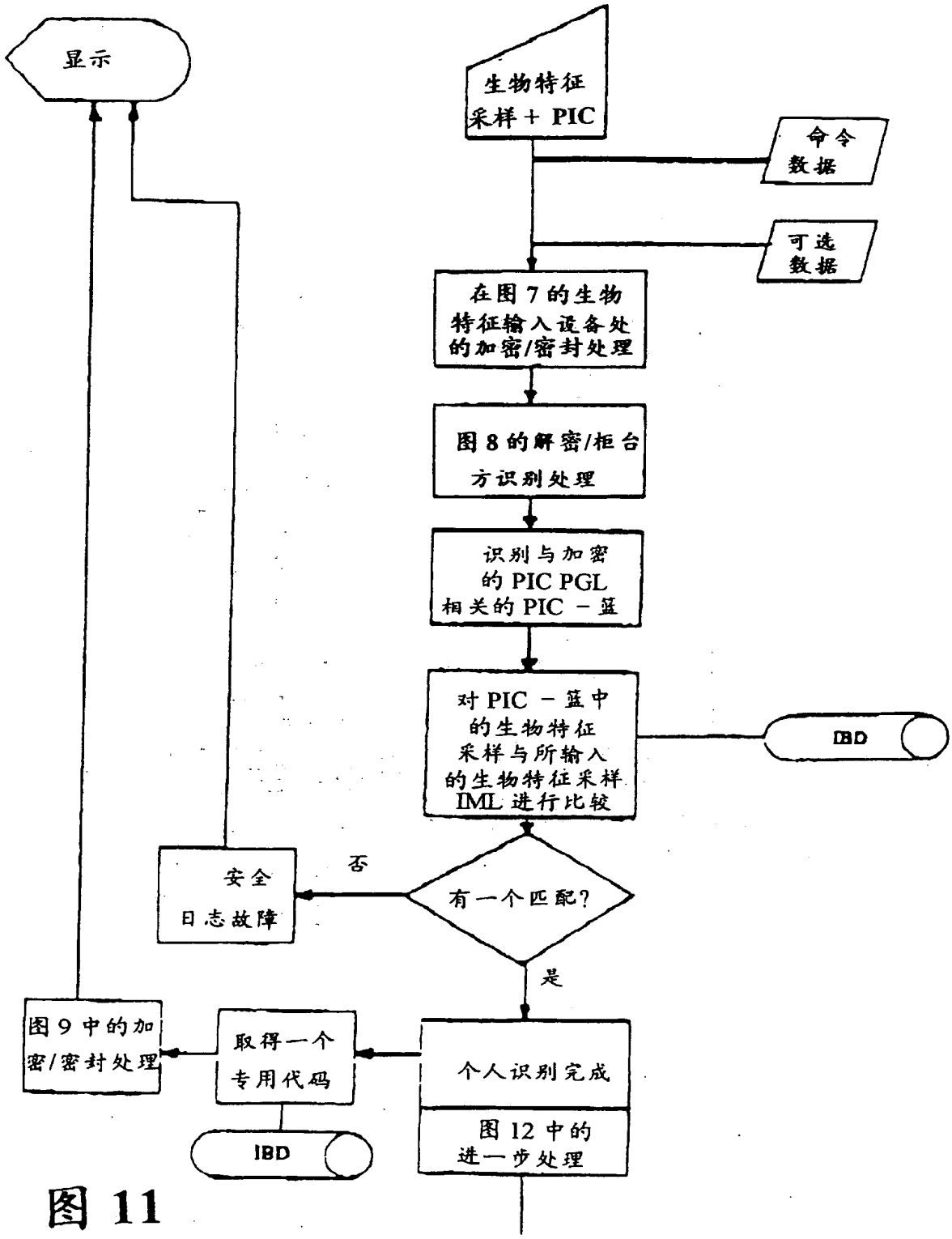

显示
生物特征
采样 + PIC
命令
数据
可选
数据
在图 7 的生物
特征输入设备处
的加密/密封处理
图 8 的解密/柜台
方识别处理
识别与加密
的 PIC PGL
相关的 PIC - 篮
对 PIC - 篮中
的生物特征
采样与所输入
的生物特征采样
IML 进行比较
IBD
否
安全
日志故障
有一个匹配?
是
图 9 中的加
密/密封处理
取得一个
专用代码
个人识别完成
IBD
图 12 中的
进一步处理

图 11

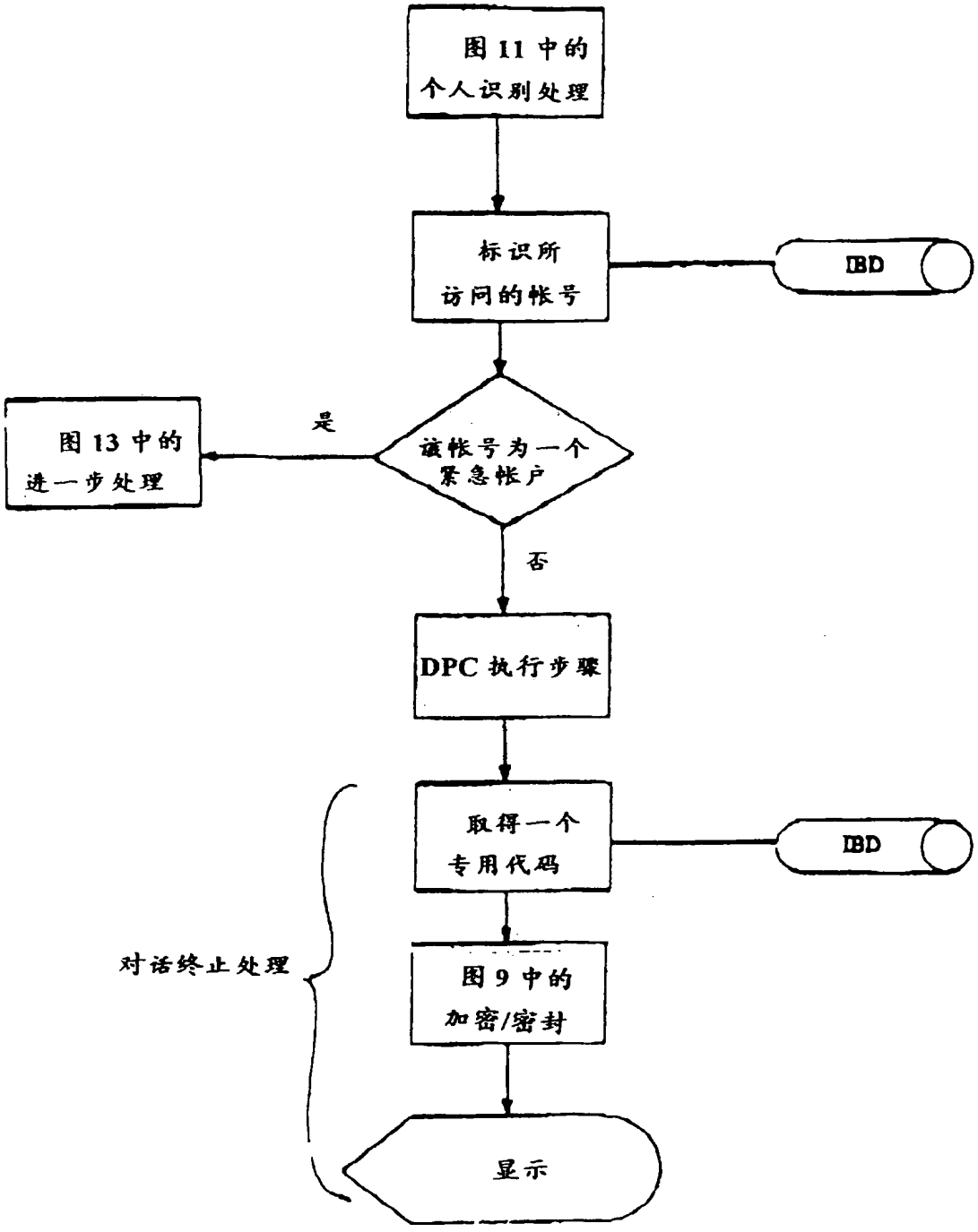


图 11 中的
个人识别处理
标识所
访问的帐号
IBD
该帐号为一个
紧急帐户
是
图 13 中的
进一步处理
否
DPC 执行步骤
取得一个
专用代码
IBD
对话终止处理
图 9 中的
加密/密封
显示

图 12

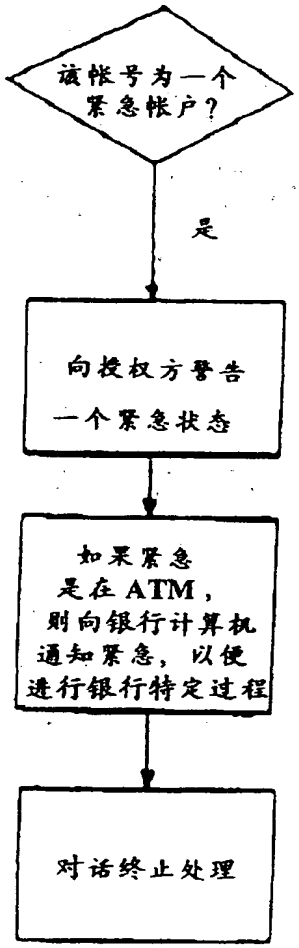

该帐号为一个
紧急帐户？
是
向授权方警告
一个紧急状态
如果紧急
是在ATM，
则向银行计算机
通知紧急，以便
进行银行特定过程
对话终止处理

图 13

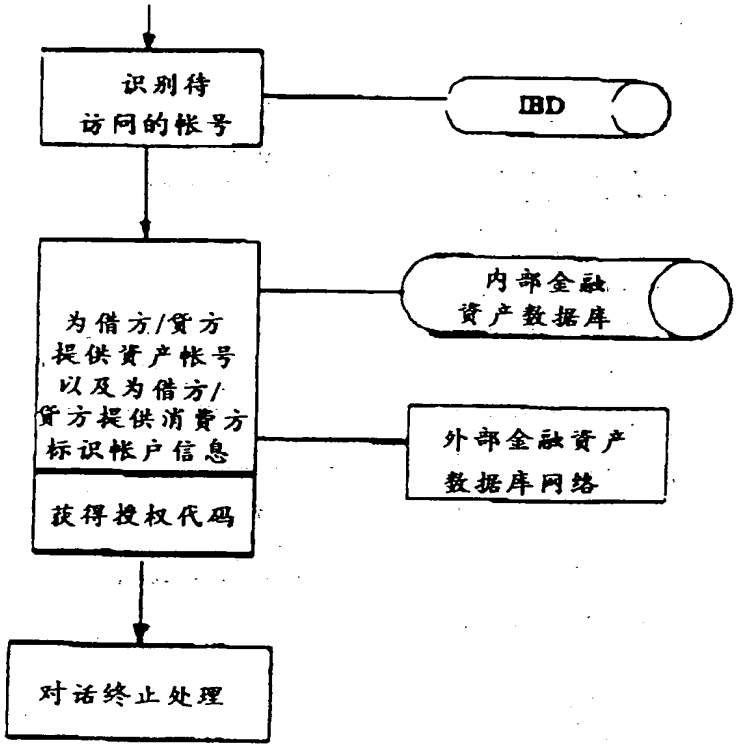

识别待
访问的帐号
IBD
为借方/贷方
提供资产帐号
以及为借方/
贷方提供消费方
标识帐户信息
内部金融
资产数据库
外部金融资产
数据库网络
获得授权代码
对话终止处理

图 14

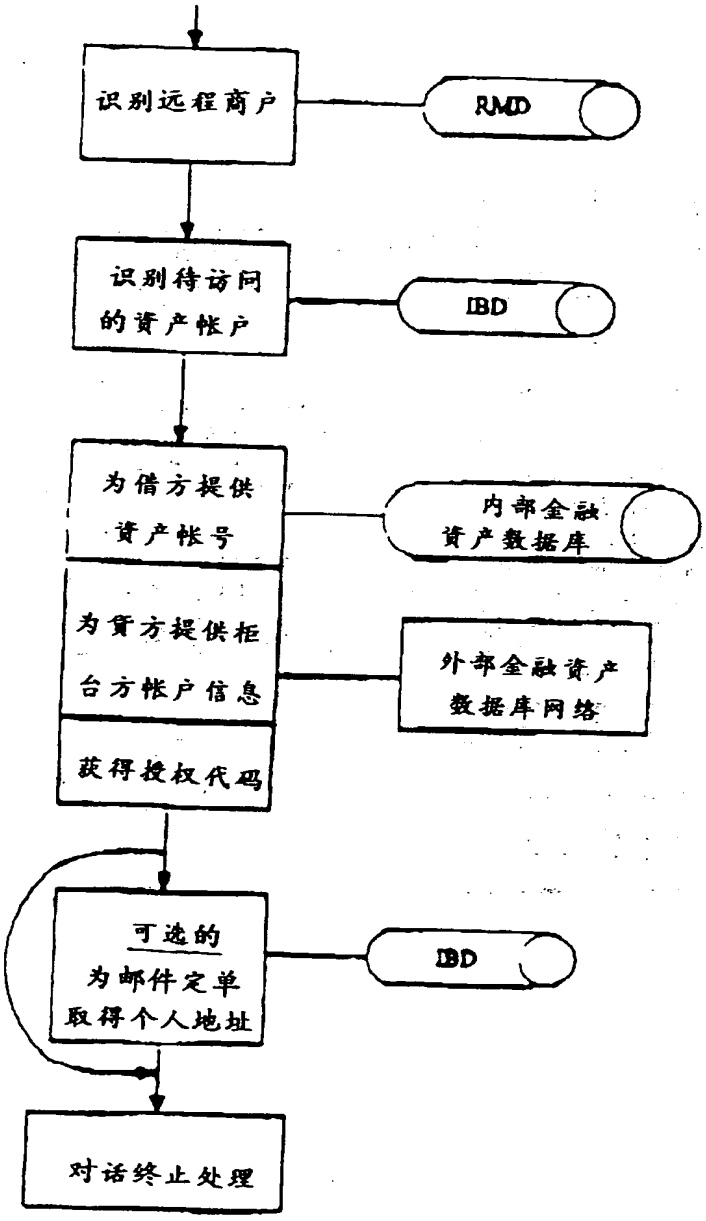

识别远程商户
RMD
识别待访问的资产帐户
IBD
为借方提供资产帐号
内部金融资产数据库
为贷方提供柜台方帐户信息
外部金融资产数据库网络
获得授权代码
可选的
为邮件定单取得个人地址
IBD
对话终止处理

图 15

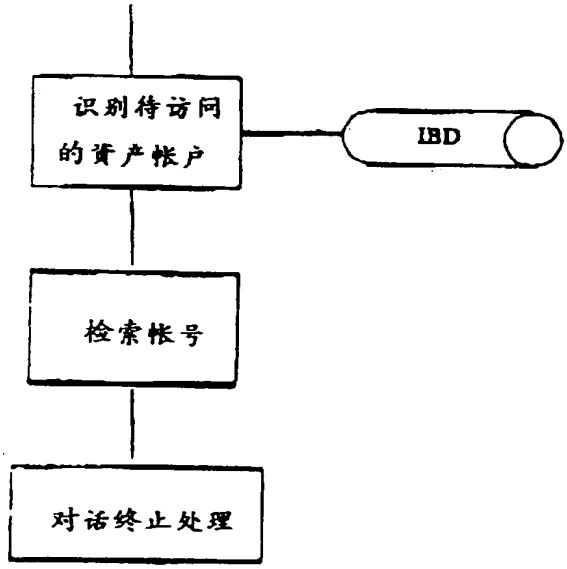


图 16

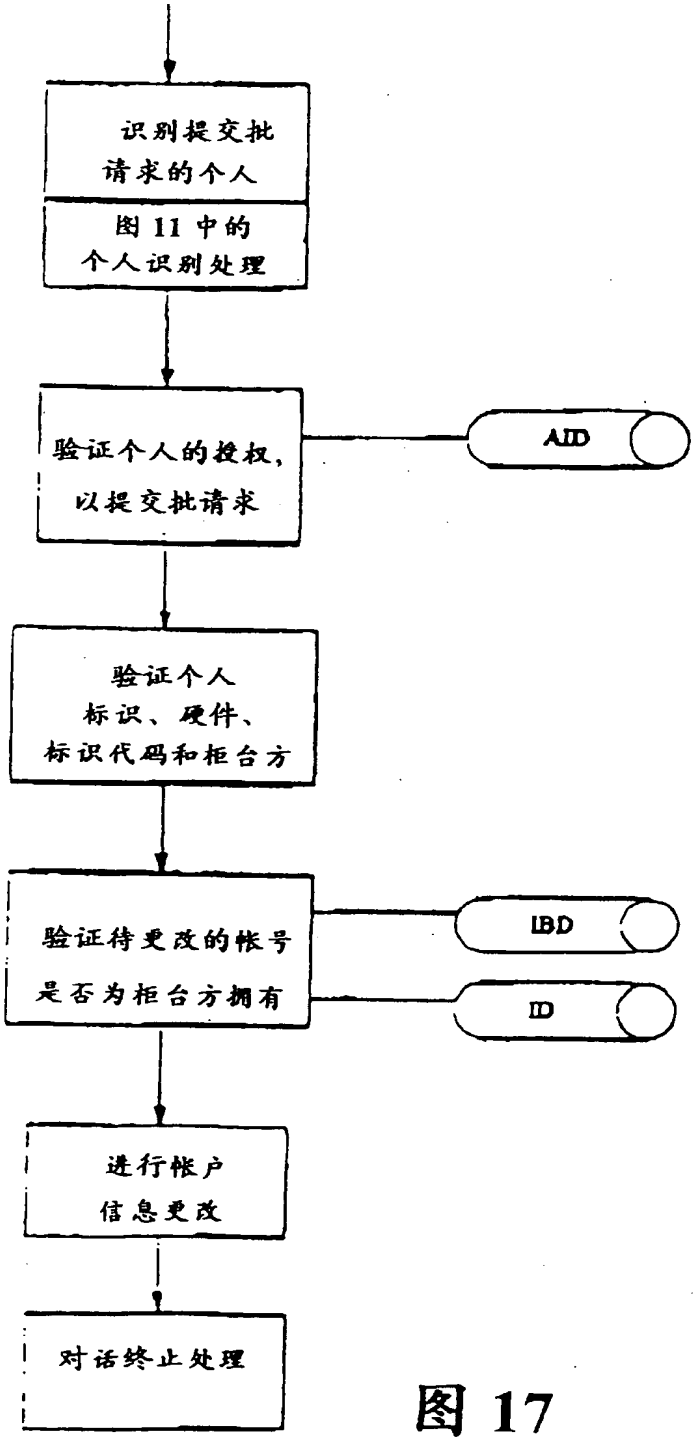

识别提交批请求的个人
图 11 中的个人识别处理
验证个人的授权，以提交批请求
AID
验证个人标识、硬件、标识代码和柜台方
验证待更改的帐号是否为柜台方拥有
IBD
ID
进行帐户信息更改
对话终止处理

图 17

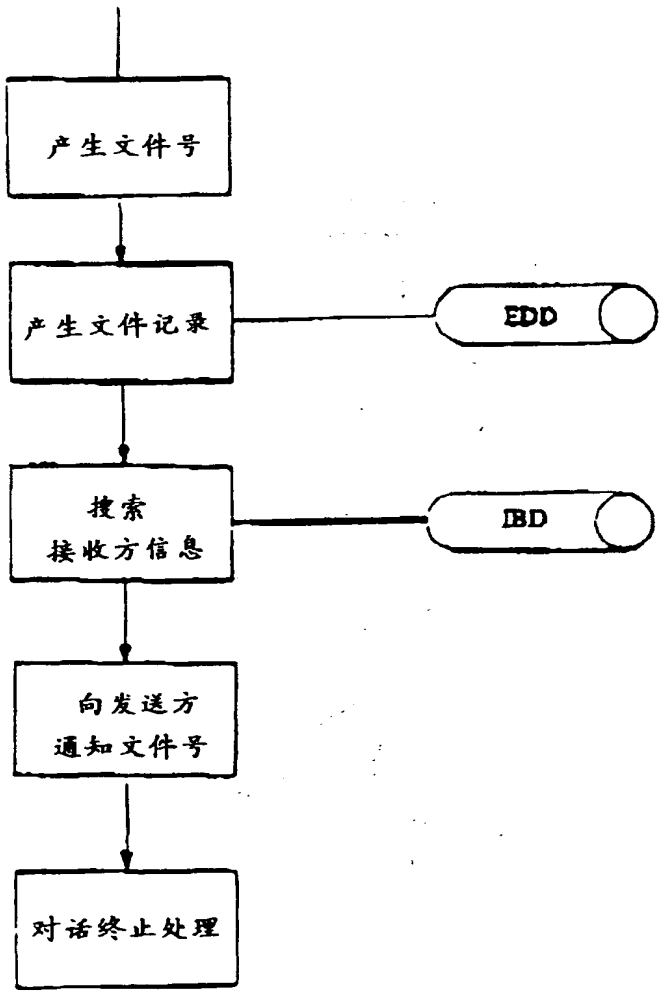


图 18

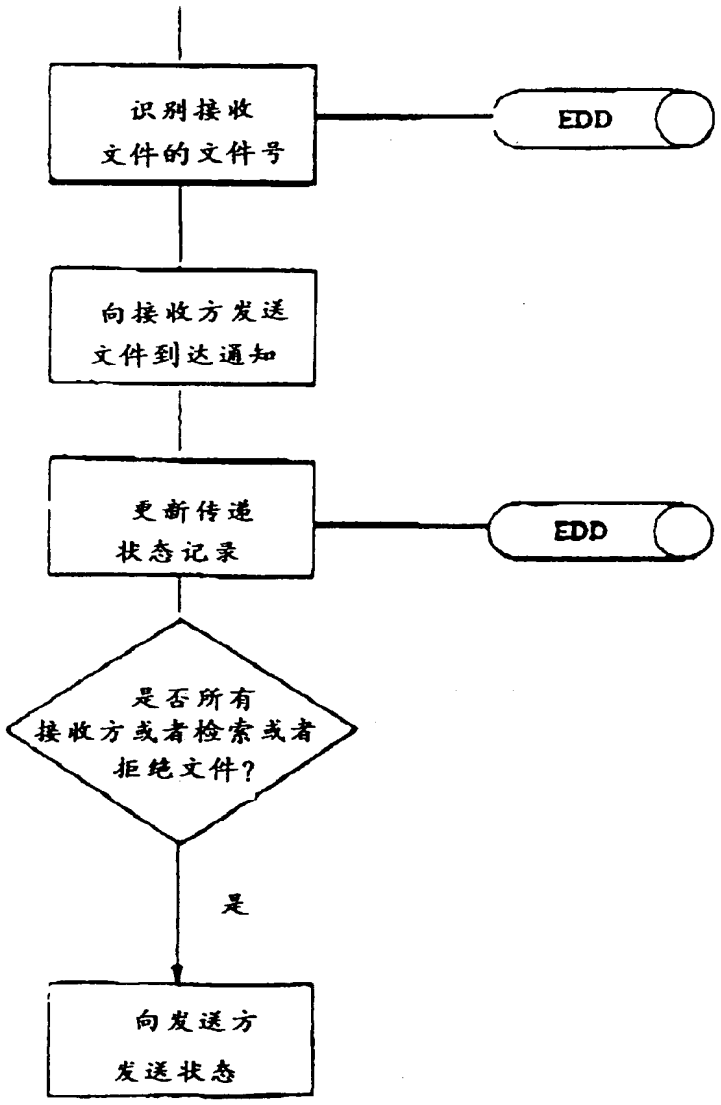

识别接收
文件的文件号
EDD
向接收方发送
文件到达通知
更新传递
状态记录
EDD
是否所有
接收方或者检索或者
拒绝文件?
是
向发送方
发送状态

图 19

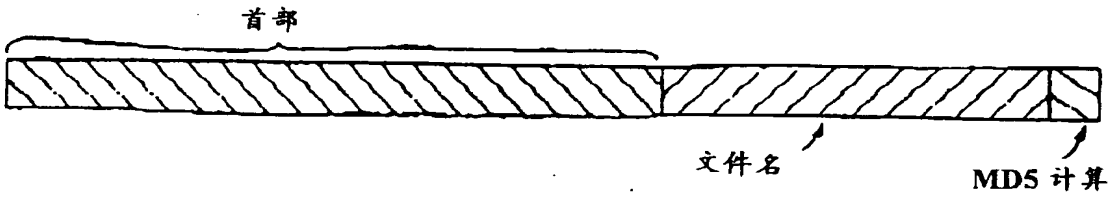


图 20A

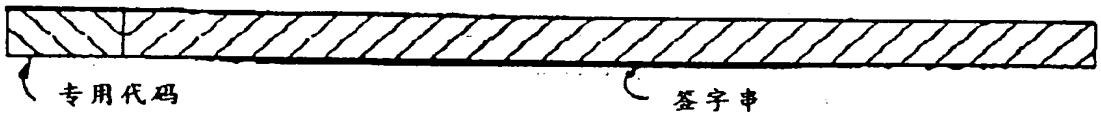


图 20B

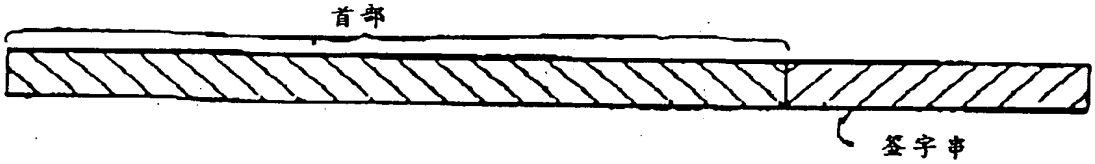


图 20C

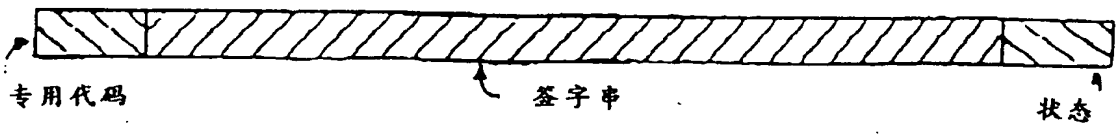


图 20D

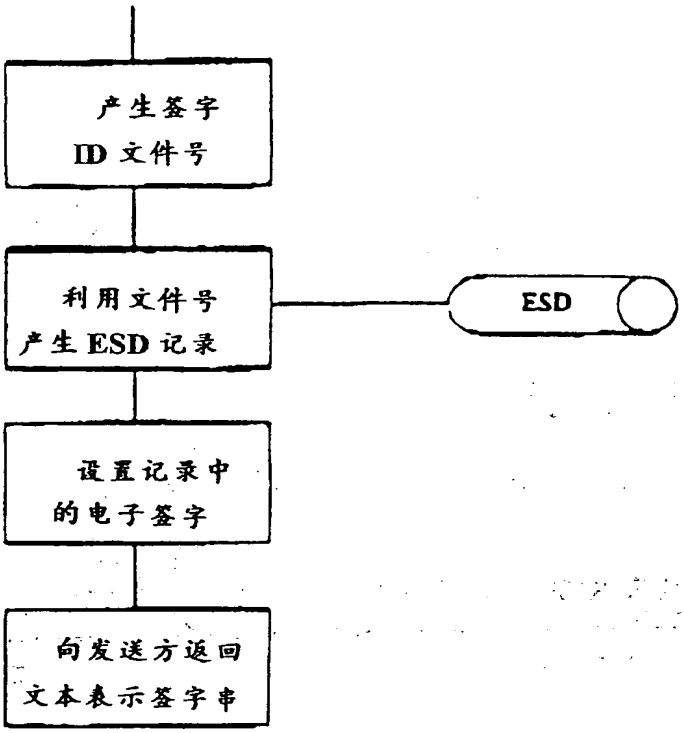

产生签字
ID 文件号
利用文件号
产生 ESD 记录
ESD
设置记录中
的电子签字
向发送方返回
文本表示签字串

图 21

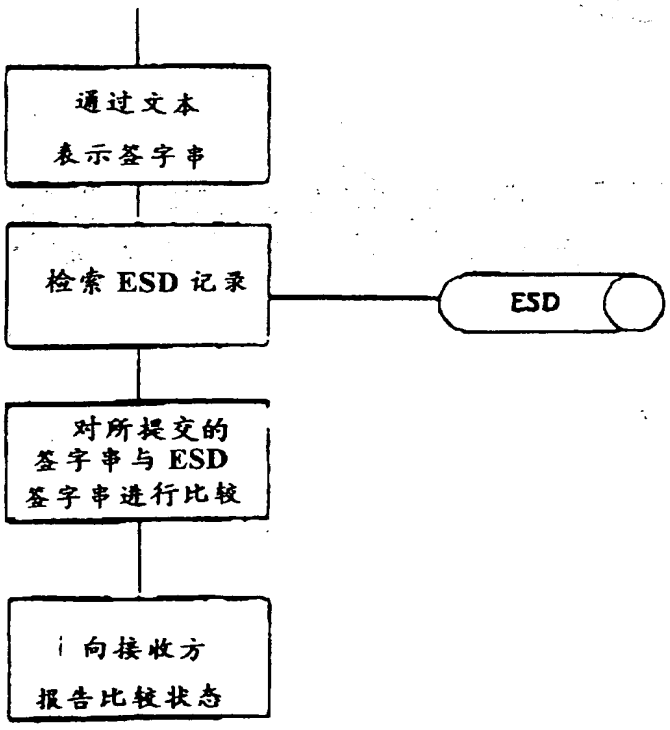

通过文本
表示签字串
检索 ESD 记录
ESD
对所提交的
签字串与 ESD
签字串进行比较
向接收方
报告比较状态

图 22